rmon collection stats

Use the **rmon collection stats** interface configuration command on the switch stack or on a standalone switch to collect Ethernet group statistics, which include utilization statistics about broadcast and multicast packets, and error statistics about Cyclic Redundancy Check (CRC) alignment errors and collisions. Use the **no** form of this command to return to the default setting.

rmon collection stats *index* [**owner** *name*]

no rmon collection stats *index* [**owner** *name*]

Syntax Description

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

Defaults

The RMON statistics collection is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

The RMON statistics collection command is based on hardware counters.

Examples

This example shows how to collect RMON statistics for the owner *root* on Gigabit Ethernet interface 0/1 of stack member 2:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# rmon collection stats 2 owner root
```

You can verify your setting by entering the **show rmon statistics** privileged EXEC command.

Related Commands

Command	Description
show rmon statistics	Displays RMON statistics. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS System Management Commands > RMON Commands**.

sdm prefer

Use the **sdm prefer** global configuration command on the switch stack or on a standalone switch to configure the template used in Switch Database Management (SDM) resource allocation. You can use a template to allocate system resources to best support the features being used in your application. Use a template to provide maximum system utilization for unicast routing or for VLAN configuration or to change an aggregator template (Catalyst 3750-12S only) to a desktop template. Use the **no** form of this command to return to the default template.

sdm prefer {**default** | **routing** | **vlan**} [**desktop**]

no sdm prefer

Syntax Description

default	Set the switch to use the default template (Catalyst 3750-12S only). This keyword is not available on switches that do not allow the aggregator template (desktop switches). On these switches, enter the **no sdm prefer** command to set the default template.
routing	Provide maximum system utilization for unicast routing. You would typically use this template for a router or aggregator in the middle of a network.
vlan	Provide maximum system utilization for VLANs. This template maximizes system resources for use as a Layer 2 switch with no routing.
desktop	Use only on a Catalyst 3750-12S switch (where aggregator templates are the default), to select the default, routing, or VLAN desktop template.

Defaults

The default template provides a balance to all features.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The aggregator templates were added.

Usage Guidelines

You must reload the switch for the configuration to take effect. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

Desktop switches support only desktop templates; an aggregator switch (Catalyst 3750-12S) supports both desktop and aggregator templates. On an aggregator switch, if you do not enter the desktop keyword, the aggregator templates are selected.

All stack members use the same SDM desktop or aggregator template, stored on the stack master. When a new switch member is added to a stack, as with the switch configuration file and VLAN database file, the SDM configuration that is stored on the stack master overrides the template configured on an individual switch.

If a stack member cannot support the template that is running on the master switch, the switch goes into SDM mismatch mode, the master switch does not attempt to change the SDM template, and the switch cannot be a functioning member of the stack.

- If the master switch is a Catalyst 3750-12S, and you change the template from an aggregator template to a desktop template and reload the switch, the entire stack operates with the selected desktop template. This could cause configuration losses if the number of ternary content addressable memory (TCAM) entries exceeds the desktop template sizes.
- If you change the template on a Catalyst 3750-12S master from a desktop template to an aggregator template and reload the switch, any desktop switches that were part of the stack go into SDM mismatch mode.
- If you add a Catalyst 3750-12S switch that is running the aggregator template to a stack that has a desktop switch as the stack master, the stack operates with the desktop template selected on the stack master. This could cause configuration losses on the Catalyst 3750-12S stack member if the number of TCAM entries on it exceeds desktop template sizes.

Note For more information about stacking, refer to the "Managing Switch Stacks" chapter in the software configuration guide.

Use the **sdm prefer vlan** [**desktop**] global configuration command only on switches intended for Layer 2 switching with no routing. When you use the VLAN template, no system resources are reserved for routing entries and any routing is done through software. This overloads the central processing unit (CPU) and severely degrades routing performance.

Do not use the routing template if you do not have routing enabled on your switch. Entering the **sdm prefer routing** [**desktop**] global configuration command prevents other features from using the memory allocated to unicast routing in the routing template.

Table 2-15 lists the approximate number of each resource supported in each of the three templates for a desktop or aggregator switch. The first eight rows in the tables (unicast MAC addresses through security ACEs) represent approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance. The last row is a guideline used to calculate hardware resource consumption related to the number of Layer 3 VLANs configured.

Table 2-15 Approximate Number of Feature Resources Allowed by Each Template

	Desktop Templates			Aggregator Templates		
Resource	**Default**	**Routing**	**VLAN**	**Default**	**Routing**	**VLAN**
Unicast MAC addresses	6 K	3 K	12 K	6 K	6 K	12 K
Internet Group Management Protocol (IGMP) groups and multicast routes	1 K	1 K	1 K	1 K	1 K	1 K
Unicast routes	8 K	11 K	0	12 K	20 K	0
• Directly connected hosts	6 K	3 K	0	6 K	6 K	0
• Indirect routes	2 K	8 K	0	6 K	14 K	0
Policy-based routing access control entries (ACEs)	0	512	0	0	512	0
QoS classification ACEs	512	512	512	896	512	896

Table 2-15 Approximate Number of Feature Resources Allowed by Each Template (continued)

Resource	Desktop Templates			Aggregator Templates		
	Default	Routing	VLAN	Default	Routing	VLAN
Security ACEs	1 K	1 K	1 K	1 K	1 K	1 K
Layer 2 VLANs	1 K	1 K	1 K	1 K	1 K	1 K

Examples

This example shows how to configure the routing template on a desktop switch:

```
Switch(config)# sdm prefer routing
Switch(config)# exit
Switch# reload
```

This example shows how to configure the desktop routing template on an aggregator switch:

```
Switch(config)# sdm prefer routing desktop
Switch(config)# exit
Switch# reload
```

This example shows how to change a switch template to the default template. On an aggregator switch, this is the default aggregator template; on a desktop switch, this is the default desktop template.

```
Switch(config)# no sdm prefer
Switch(config)# exit
Switch# reload
```

This example shows how to configure the desktop default template on an aggregator switch:

```
Switch(config)# sdm prefer default desktop
Switch(config)# exit
Switch# reload
```

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

Related Commands

Command	Description
show sdm prefer	Displays the current SDM template in use or displays the templates that can be used, with approximate resource allocation per feature.

service password-recovery

Use the **service password-recovery** global configuration command on the switch stack or on a standalone switch 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

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)AX	This command was first introduced.

Usage Guidelines

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 is displayed:

```
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.

When you enter the **service password-recovery** or **no service password-recovery** command on the stack master, it is propagated throughout the stack and applied to all switches in the stack.

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 or switch stack 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 on the switch stack or on a standalone switch 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*

Syntax Description

input *policy-map-name*	Apply the specified policy-map to the input of an interface.

Note Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics it gathers. The **output** keyword is also not supported.

Defaults

No policy maps are attached to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

Only one policy map per ingress interface is supported.

Classification using a port trust state (for example, **mls qos trust** [**cos** | **dscp** | **ip-precedence**] and a policy map (for example, **service-policy input** *policy-map-name*) are mutually exclusive. The last one configured overwrites the previous configuration.

Examples

This example shows how to apply *plcmap1* to an ingress interface on stack member 2:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input plcmap1
```

This example shows how to detach *plcmap2* from an interface on stack member 2:

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# no service-policy input plcmap2
```

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

session

Use the **session** privileged EXEC command on the stack master to access a specific stack member.

session *stack-member-number*

Syntax Description

stack-member-number	Specify the current stack member number. The stack member number is in the range from 1 through 9.

Defaults

No default is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

When you access the stack member, its stack member number is appended to the system prompt.

Examples

This example shows how to access stack member 6:

```
Switch(config)# session 6
Switch-6#
```

Related Commands

Command	Description
reload	Saves the configuration change and restarts the stack member.
switch priority	Changes the stack member priority value.
switch renumber	Changes the stack member number.
show switch	Displays information about the switch stack and its stack members.

set

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

set {**ip dscp** *new-dscp* | **ip precedence** *new-precedence*}

no set {**ip dscp** *new-dscp* | **ip precedence** *new-precedence*}

Syntax Description

ip dscp *new-dscp*	New DSCP value assigned to the classified traffic. The range is 0 to 63. You also can enter a mnemonic name for a commonly-used value.
ip precedence *new-precedence*	New IP-precedence value assigned to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly-used value.

Note Though visible in the command-line help strings, the **mpls** keyword is not supported.

Defaults

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

The **set** command is mutually exclusive with the **trust** policy-map class configuration command within the same policy map.

For the **set ip dscp** *new-dscp* or the **set ip precedence** *new-precedence* command, you can enter a mnemonic name for a commonly-used value. For example, you can enter the **set ip dscp af11** command, which is the as same entering the **set ip dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set ip dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

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

Examples

This example shows how to assign DSCP 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
class	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
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.
trust	Defines a trust state for traffic classified through the **class** policy-map configuration command or the **class-map** global configuration command.

setup

Use the setup privileged EXEC command to configure the switch with its initial configuration.

setup

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

When you use the **setup** command, make sure that you have this information:

- IP address and network mask
- Password strategy for your environment
- Whether the switch will be used as the cluster command switch and the cluster name

When you enter the **setup** command, an interactive dialog, called the System Configuration Dialog, appears. It guides you through the configuration process and prompts you for information. The values shown in brackets next to each prompt are the default values last set by using either the **setup** command facility or the **configure** privileged EXEC command.

Help text is provided for each prompt. To access help text, press the question mark (**?**) key at a prompt.

To return to the privileged EXEC prompt without making changes and without running through the entire System Configuration Dialog, press **Ctrl-C**.

When you complete your changes, the setup program shows you the configuration command script that was created during the setup session. You can save the configuration in nonvolatile RAM (NVRAM), return to the setup program without saving, or return to the command-line prompt without saving the configuration.

Examples

This is an example of output from the **setup** command:

```
Switch# setup

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

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

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Switch]:host-name

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: enable-secret-password

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: enable-password

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: terminal-password

  Configure SNMP Network Management? [no]: yes
  Community string [public]:

Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      172.20.135.202  YES NVRAM  up                    up

GigabitEthernet6/0/1         unassigned      YES unset  up                      up

GigabitEthernet6/0/2         unassigned      YES unset  up                      down

GigabitEthernet6/0/3         unassigned      YES unset  administratively down down

GigabitEthernet6/0/4         unassigned      YES unset  up                      down

GigabitEthernet6/0/5         unassigned      YES NVRAM  up                      down

GigabitEthernet6/0/6         unassigned      YES NVRAM  up                      down

GigabitEthernet6/0/7         unassigned      YES unset  up                      down

GigabitEthernet6/0/8         unassigned      YES unset  up                      down

GigabitEthernet6/0/9         unassigned      YES unset  administratively down down

GigabitEthernet6/0/10        10.1.2.3        YES NVRAM  up                      down
```

```
GigabitEthernet6/0/11        unassigned      YES unset  up                    down

GigabitEthernet6/0/12        unassigned      YES unset  up                    down

Port-channel1              unassigned      YES unset  up                    down

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: ip_address
Subnet mask for this interface [255.0.0.0]: subnet_mask

Would you like to enable as a cluster command switch? [yes/no]: yes

Enter cluster name: cluster-name

The following configuration command script was created:

hostname host-name
enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet6/0/1
no ip address
!
interface GigabitEthernet6/0/2
no ip address
!
...
interface GigabitEthernet6/0/12
no ip address

cluster enable cluster-name
!
end
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands**.
show version	Displays version information for the hardware and firmware.

setup express

Use the **setup express** global configuration command to enable Express Setup mode on the switch stack or on a standalone switch. Use the **no** form of this command to disable Express Setup mode.

setup express

no setup express

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 first 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 flashing. 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 turn solid green after 3 seconds.
- On a configured switch, the mode LEDs begin flashing after 2 seconds and turn solid green after 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 do not turn solid green *or* begin flashing green if Express Setup mode is not enabled on the switch.

Related Commands

Command	Description
clear setup express	Exits Express Setup mode.
show setup express	Displays if Express Setup mode is active.

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* | **hardware counters** | **ipc**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

name	(Optional) Name of the ACL.
number	(Optional) ACL number. The range is 1 to 2699.
hardware counters	(Optional) Display global hardware ACL statistics for switched and routed packets.
ipc	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help strings, the **rate-limit** keywords are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **ipc** keyword was added.

Usage Guidelines

The switch supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2699.

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

Examples

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

```
Switch# show access-lists
Standard IP access list 1
    permit 1.1.1.1
    permit 2.2.2.2
    permit any
    permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
    permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
    permit 10.10.10.10
Extended IP access list 121
    permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
Extended IP access list CMP-NAT-ACL
    Dynamic Cluster-HSRP deny   ip any any
      deny ip any host 19.19.11.11
      deny ip any host 10.11.12.13
    Dynamic Cluster-NAT permit ip any any
      permit ip host 10.99.100.128 any
      permit ip host 10.46.22.128 any
      permit ip host 10.45.101.64 any
      permit ip host 10.45.20.64 any
      permit ip host 10.213.43.128 any
      permit ip host 10.91.28.64 any
      permit ip host 10.99.75.128 any
      permit ip host 10.38.49.0 any
```

This is an example of output from the **show access-lists hardware counters** command:

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
     Drop:                All frame count: 855
     Drop:                All bytes count: 94143
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 2121
     Forwarded:           All bytes count: 180762
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L3 ACL INPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 13586
     Forwarded:           All bytes count: 1236182
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0
```

```
L2 ACL OUTPUT Statistics
    Drop:                All frame count: 0
    Drop:                All bytes count: 0
    Drop And Log:        All frame count: 0
    Drop And Log:        All bytes count: 0
    Bridge Only:         All frame count: 0
    Bridge Only:         All bytes count: 0
    Bridge Only And Log: All frame count: 0
    Bridge Only And Log: All bytes count: 0
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 232983
    Forwarded:           All bytes count: 16825661
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0

L3 ACL OUTPUT Statistics
    Drop:                All frame count: 0
    Drop:                All bytes count: 0
    Drop And Log:        All frame count: 0
    Drop And Log:        All bytes count: 0
    Bridge Only:         All frame count: 0
    Bridge Only:         All bytes count: 0
    Bridge Only And Log: All frame count: 0
    Bridge Only And Log: All bytes count: 0
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 514434
    Forwarded:           All bytes count: 39048748
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0
```

Related Commands

Command	Description
access-list	Configures a standard or extended numbered access list on the switch. For syntax information, select **Cisco IOS IP and IP Routing Command Reference for IOS Release 12.1 > IP Addressing and Services > IP Services Commands**.
ip access list	Configures a named IP access list on the switch. For syntax information, select **Cisco IOS IP and IP Routing Command Reference for IOS Release 12.1 > IP Addressing and Services > IP Services Commands**.
mac access-list extended	Configures a named or numbered MAC access list on the switch.

show auto qos

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

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

Syntax Description

interface [*interface-id*]	(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 *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

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

Usage Guidelines

The **show auto qos** [**interface** [*interface-id*]] command displays the initial auto-QoS configuration; it does not display any user changes to the configuration that might be in effect. Use the **show running-config** privileged EXEC command to display the auto-QoS configuration and the user modifications.

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 maps cos-dscp**
- **show mls qos interface** [*interface-id*] [**buffers** | **queueing**]
- **show mls qos maps** [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-output-q**]
- **show mls qos input-queue**
- **show running-config**

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

Examples

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

```
Switch# show auto qos
Initial configuration applied by AutoQoS:
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos
no mls qos srr-queue input cos-map
no mls qos srr-queue output cos-map
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
no mls qos srr-queue input dscp-map
no mls qos srr-queue output dscp-map
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 26 33 34 35 36 37 38 39
mls qos srr-queue input dscp-map queue 2 threshold 2 48 49 50 51 52 53 54 55
mls qos srr-queue input dscp-map queue 2 threshold 2 56 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 27 28 29 30 31 40
mls qos srr-queue input dscp-map queue 2 threshold 3 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
no mls qos srr-queue input priority-queue 1
no mls qos srr-queue input priority-queue 2
mls qos srr-queue input bandwidth 90 10
no mls qos srr-queue input buffers
mls qos queue-set output 1 buffers 20 20 20 40
!
interface GigabitEthernet2/0/2
 mls qos trust device cisco-phone
 mls qos trust cos
 no queue-set 1
 srr-queue bandwidth shape 10 0 0 0
 srr-queue bandwidth share 10 10 60 20
```

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

```
Switch# show auto qos interface
Initial configuration applied by AutoQoS:
!
interface GigabitEthernet2/0/2
 mls qos trust device cisco-phone
 mls qos trust cos
 no queue-set 1
 srr-queue bandwidth shape 10 0 0 0
 srr-queue bandwidth share 10 10 60 20
```

This is an example of output from the **show auto qos interface gigabitethernet2/0/2** command after the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface gigabitethernet2/0/2
 mls qos trust device cisco-phone
 mls qos trust cos
 no queue-set 1
 srr-queue bandwidth shape 10 0 0 0
 srr-queue bandwidth share 10 10 60 20
```

Related Commands

Command	Description
auto qos voip	Automatically configures QoS for VoIP within a QoS domain.
debug autoqos	Enables debugging of the auto-QoS feature.

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show boot** command. Table 2-16 describes each field in the display.

```
Switch# show boot
BOOT path-list:      flash:c29703750-i5q3l2-mz-121.11.AX/c29703750-i5q3l2-mz-121.11.AX.bin
Config file:         flash:config.text
Private Config file: private-config
Enable Break:        no
Manual Boot:         yes
HELPER path-list:
Auto upgrade        : yes
NVRAM/Config file
      buffer size:   32768
```

Table 2-16 show boot Field Descriptions

Field	Description
BOOT path-list	Displays a semicolon separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the Flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the Flash file system.
Config file	Displays the filename that IOS uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that IOS uses to read and write a nonvolatile copy of the system configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to yes, on, or 1, 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 no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
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.
Auto upgrade	Displays whether the switch stack is set to automatically copy its software version to an incompatible switch so that it can join the stack. A switch in version-mismatch (VM) mode is a switch that has a different stack protocol version than the version on the switch stack. Switches in VM mode cannot join the switch stack. If the switch stack has an image that can be copied to a switch in VM mode, and if the **boot auto-copy-sw** feature is enabled, the switch stack automatically copies the image from another stack member to the switch in VM mode. The switch then exits VM mode, reboots, and joins the switch stack.
NVRAM/Config file buffer size	Displays the buffer size that IOS uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation.

Related Commands

Command	Description
boot auto-copy-sw	Automatically upgrade switches in version-mismatch (VM) mode with the switch stack image.
boot config-file	Specifies the filename that IOS uses to read and write a nonvolatile copy of the system configuration.
boot enable-break	Enables interrupting the automatic boot process.
boot manual	Enables manually booting the switch during the next boot cycle.
boot private-config-file	Specifies the filename that IOS uses to read and write a nonvolatile copy of the private configuration.
boot system	Specifies the IOS image to load during the next boot cycle.

show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** privileged EXEC command to display the Time Domain Reflector (TDR) results.

show cable-diagnostics tdr interface *interface-id* [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

TDR is supported only on copper Ethernet 10/100/1000 ports. It is not supported on 10/100 ports or small form-factor pluggable (SFP) module ports. For more information about TDR, refer to the software configuration guide for this release

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

Examples

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command:

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi1/0/2   auto  Pair A     0    +/- 2  meters N/A         Open
                Pair B     0    +/- 2  meters N/A         Open
                Pair C     0    +/- 2  meters N/A         Open
                Pair D     0    +/- 2  meters N/A         Open
```

Table 2-17 lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

Table 2-17 Fields Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	Interface on which TDR was run.
Speed	Current speed of connection.
Local pair	Name of the pair of wires that TDR is testing on the local interface.

Table 2-17 Fields Descriptions for the show cable-diagnostics tdr Command Output (continued)

Field	Description
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can determine the location only in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 1000 Mbps. • The cable is open • The cable has a short.
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can determine the remote pair only when the cable is connected properly and the link is up.
Pair status	The status of the pair of wires on which TDR is running: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted.

For more examples of output from the **show cable-diagnostics tdr interface** *interface-id* command, refer to the software configuration guide for this release.

Related Commands

Command	Description
test cable-diagnostics tdr	Enables and runs TDR on an interface.

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*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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

```
Switch> show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all dscp5 (id 3)
   Match ip dscp 5
```

Related Commands

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

show cluster

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

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

On a cluster command switch stack or cluster 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.

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

Examples

This is an example of output when the **show cluster** command is entered on the active cluster command switch:

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

This is an example of output when the **show cluster** command is entered on a cluster member switch:

```
Switch1> show cluster
Member switch for cluster "hapuna"
        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 the **show cluster** command is entered on a cluster member switch that is configured as the standby cluster command switch:

```
Switch> show cluster
Member switch for cluster "hapuna"
        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 the **show cluster** command is entered on the cluster command switch that has lost connectivity with member 1:

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

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

```
Switch> show cluster
Member switch for cluster "hapuna"
        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 a switch stack or on a cluster command switch to display a list of candidate switches.

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

This command is available only on the cluster command switch stack or cluster command switch.

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

The SN in the display means *switch member number*. If E appears 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 cluster command switch.

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

Examples

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 StLouis-2    WS-C37502970-12T     Gi6/0/1       2   1  Fa0/11
       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 Surfers-24   WS-C2924-XL      Fa0/5        1   0  Fa0/3
       00e0.1e9f.8c00 Surfers-12-2 WS-C2912-XL      Fa0/4        1   0  Fa0/7
       00e0.1e9f.8c40 Surfers-12-1 WS-C2912-XL      Fa0/1        1   0  Fa0/9
```

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

```
Switch> show cluster candidates mac-address 00d0.7961.c4c0
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C37502970-12T
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 0)
        Local port:             Gi6/0/1   FEC number:
        Upstream port:          GI6/0/11  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 cluster member switch three hops from the cluster edge:

```
Switch> show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
        Device type:            cisco WS-C2912MF-XL
        Upstream MAC address:   0010.7bb6.1cd4
        Local port:             Fa2/1   FEC number:
        Upstream port:          Fa0/24  FEC Number:
        Hops from cluster edge: 3
        Hops from command device: -
```

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

```
Switch> show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C3512-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 1)
        Local port:             Fa0/3   FEC number:
        Upstream port:          Fa0/13  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
    Device '1900_Switch' with mac address number 00e0.1e7e.be80
        Device type:            cisco 1900
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 2)
        Local port:             3       FEC number: 0
        Upstream port:          Fa0/11  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
        Device type:            cisco WS-C2924-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 3)
        Local port:             Fa0/5   FEC number:
        Upstream port:          Fa0/3   FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
```

Related Commands

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

show cluster members

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

This command is available only on the cluster command switch stack or cluster command switch.

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

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

Examples

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

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

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

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
        Device type:            cisco WS-C37502970-12T
        MAC address:            0002.4b29.4400
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi6/0/1   FEC number:
        Upstream port:          GI6/0/11  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-C37502970-12T
        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-C37502970-12T
        MAC address:            0002.4b29.4400
        Upstream MAC address:   0030.946c.d740 (Cluster member 1)
        Local port:             Gi6/0/1   FEC number:
        Upstream port:          Fa6/0/11  FEC Number:
        Hops from command device: 2
Device 'GenieTest' 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 cpu-interface

Use the **show controllers cpu-interface** privileged EXEC command to display the state of the CPU network interface application-specific integrated circuit (ASIC) and the send and receive statistics for packets reaching the CPU.

show controllers cpu-interface [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

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

Examples

This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped    invalid    hol-block
----------------- ---------- ---------- ---------- ----------
rpc               4523063    0          0          0
stp               1545035    0          0          0
ipc               1903047    0          0          0
routing protocol  96145      0          0          0
L2 protocol       79596      0          0          0
remote console    0          0          0          0
sw forwarding     5756       0          0          0
host              225646     0          0          0
broadcast         46472      0          0          0
cbt-to-spt        0          0          0          0
igmp snooping     68411      0          0          0
icmp              0          0          0          0
logging           0          0          0          0
rpf-fail          0          0          0          0
queue14           0          0          0          0
cpu heartbeat     1710501    0          0          0
```

```
Supervisor ASIC receive-queue parameters
----------------------------------------
 queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
 queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
 queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
 queue 3 maxrecevsize 5EE pakhead 19CDDD0 paktail 19D02C8

<output truncated>

Supervisor ASIC Mic Registers
-----------------------------
MicDirectPollInfo               80000800
MicIndicationsReceived          00000000
MicInterruptsReceived           00000000
MicPcsInfo                      0001001F
MicPlbMasterConfiguration       00000000
MicRxFifosAvailable             00000000
MicRxFifosReady                 0000BFFF
MicTimeOutPeriod:       FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000

<output truncated>

MicTransmitFifoInfo:
Fifo0:    StartPtrs:     038C2800        ReadPtr:        038C2C38
         WritePtrs:      038C2C38        Fifo_Flag:      8A800800
         Weights:        001E001E
Fifo1:   StartPtr:       03A9BC00        ReadPtr:        03A9BC60
         WritePtrs:      03A9BC60        Fifo_Flag:      89800400
         writeHeaderPtr: 03A9BC60
Fifo2:   StartPtr:       038C8800        ReadPtr:        038C88E0
         WritePtrs:      038C88E0        Fifo_Flag:      88800200
         writeHeaderPtr: 038C88E0
Fifo3:   StartPtr:       03C30400        ReadPtr:        03C30638
         WritePtrs:      03C30638        Fifo_Flag:      89800400
         writeHeaderPtr: 03C30638
Fifo4:   StartPtr:       03AD5000        ReadPtr:        03AD50A0
         WritePtrs:      03AD50A0        Fifo_Flag:      89800400
         writeHeaderPtr: 03AD50A0
Fifo5:   StartPtr:       03A7A600        ReadPtr:        03A7A600
         WritePtrs:      03A7A600        Fifo_Flag:      88800200
         writeHeaderPtr: 03A7A600
Fifo6:   StartPtr:       03BF8400        ReadPtr:        03BF87F0
         WritePtrs:      03BF87F0        Fifo_Flag:      89800400

<output truncated>
```

Related Commands

Command	Description
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

show controllers ethernet-controller

Use the **show controllers ethernet-controller** privileged EXEC command without keywords to display per-interface send and receive statistics read from the hardware. Use with the **phy** keyword to display the interface internal registers or the port-asic keyword to display information about the port application-specific integrated circuit (ASIC).

show controllers ethernet-controller [*interface-id*] [**phy**[**detail**]] **[port-asic** {**configuration | statistics**}] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	The physical interface (including type, stack member, module, and port number).
phy	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the device or the interface. This display includes the operational state of the automatic media-dependent-interface crossover (Auto MDIX) feature on an interface.
detail	(Optional) Display details about the PHY internal registers.
port-asic	(Optional) Display information about the port ASIC internal registers.
configuration	Display port ASIC internal register configuration.
statistics	Display port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

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

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

This display without keywords provides traffic statistics, basically the RMON statistics for all interfaces or for the specified interface.

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

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

Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface. Table 2-18 describes the *Transmit* fields, and Table 2-19 describes the *Receive* fields.

```
Switch# show controllers ethernet-controller GigabitEthernet6/0/1

  Transmit GigabitEthernet6/0/1              Receive
         0 Bytes                               0 Bytes
         0 Unicast frames                      0 Unicast frames
         0 Multicast frames                    0 Multicast frames
         0 Broadcast frames                    0 Broadcast frames
         0 Too old frames                      0 Unicast bytes
         0 Deferred frames                     0 Multicast bytes
         0 MTU exceeded frames                 0 Broadcast bytes
         0 1 collision frames                  0 Alignment errors
         0 2 collision frames                  0 FCS errors
         0 3 collision frames                  0 Oversize frames
         0 4 collision frames                  0 Undersize frames
         0 5 collision frames                  0 Collision fragments
         0 6 collision frames
         0 7 collision frames                  0 Minimum size frames
         0 8 collision frames                  0 65 to 127 byte frames
         0 9 collision frames                  0 128 to 255 byte frames
         0 10 collision frames                 0 256 to 511 byte frames
         0 11 collision frames                 0 512 to 1023 byte frames
         0 12 collision frames                 0 1024 to 1518 byte frames
         0 13 collision frames                 0 Overrun frames
         0 14 collision frames                 0 Pause frames
         0 15 collision frames                 0 Symbol error frames
         0 Excessive collisions
         0 Late collisions                     0 Invalid frames, too large
         0 VLAN discard frames                 0 Valid frames, too large
         0 Excess defer frames                 0 Invalid frames, too small
         0 64 byte frames                      0 Valid frames, too small
         0 127 byte frames
         0 255 byte frames                     0 Too old frames
         0 511 byte frames                     0 Valid oversize frames
         0 1023 byte frames                    0 System FCS error frames
         0 1518 byte frames                    0 RxPortFifoFull drop frame
         0 Too large frames
         0 Good (1 coll) frames
```

Table 2-18 Transmit Field Descriptions

Field	Description
Bytes	The total number of bytes transmitted on an interface.
Unicast Frames	The total number of frames transmitted to unicast addresses.
Multicast frames	The total number of frames transmitted to multicast addresses.
Broadcast frames	The total number of frames transmitted to broadcast addresses.
Too old frames	The number of frames dropped on the egress port because the packet is aged out.
Deferred frames	The number of frames that are not transmitted after the time exceeds 2*maximum-packet time.
MTU exceeded frames	The number of frames that are larger than the maximum allowed frame size.
1 collision frames	The number of frames that are successfully transmitted on an interface after one collision occurs.
2 collision frames	The number of frames that are successfully transmitted on an interface after two collisions occur.
3 collision frames	The number of frames that are successfully transmitted on an interface after three collisions occur.
4 collision frames	The number of frames that are successfully transmitted on an interface after four collisions occur.

Table 2-18 Transmit Field Descriptions (continued)

Field	Description
5 collision frames	The number of frames that are successfully transmitted on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully transmitted on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully transmitted on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully transmitted on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully transmitted on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully transmitted on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully transmitted on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully transmitted on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully transmitted on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully transmitted on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully transmitted on an interface after 15 collisions occur.
Excessive collisions	The number of frames that could not be transmitted on an interface because 16 collisions occurred.
Late collisions	After a frame is transmitted, the number of of frames dropped because late collisions were detected while the frame was transmitted.
VLAN discard frames	The number of frames dropped on an interface because the CFI[1] bit is set.
Excess defer frames	The number of frames that are not transmitted after the time exceeds the maximum-packet time.
64 byte frames	The total number of frames transmitted on an interface that are 64 bytes.
127 byte frames	The total number of frames transmitted on an interface that are from 65 to 127 bytes.
255 byte frames	The total number of frames transmitted on an interface that are from 128 to 255 bytes.
511 byte frames	The total number of frames transmitted on an interface that are from 256 to 511 bytes.
1023 byte frames	The total number of frames transmitted on an interface that are from 512 to 1023 bytes.
1518 byte frames	The total number of frames transmitted on an interface that are from 1024 to 1518 bytes.
Too large frames	The number of frames transmitted on an interface that are larger than the maximum allowed frame size.
Good (1 coll) frames	The number of frames that are successfully transmitted on an interface after one collision occurs. This value does not include the number of frames that are not successfully transmitted after one collision occurs.

1. CFI = Canonical Format Indicator

Table 2-19 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.
Unicast frames	The total number of frames successfully received on the interface that are directed to unicast addresses.
Multicast frames	The total number of frames successfully received on the interface that are directed to multicast addresses.

Table 2-19 Receive Field Descriptions (continued)

Field	Description
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly-formed frames. This value excludes the frame header bits.
Multicast bytes	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly-formed frames. This value excludes the frame header bits.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly-formed frames. This value excludes the frame header bits.
Alignment errors	The total number of frames received on an interface that have alignment errors.
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.
Oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size.
Undersize frames	The number of frames received on an interface that are smaller than 64 bytes.
Collision fragments	The number of collision fragments received on an interface.
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.
Overrun frames	The total number of overrun frames received on an interface.
Pause frames	The number of pause frames received on an interface.
Symbol error frames	The number of frames received on an interface that have symbol errors.
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 have either an FCS error or an alignment error.
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 have either an FCS error or an alignment error.
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.
Too old frames	The number of frames dropped on the ingress port because the packet is aged out.
Valid oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag.

Table 2-19 Receive Field Descriptions (continued)

Field	Description
System FCS error frames	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
RxPortFifoFull drop frames	The total number of frames received on an interface that are dropped because the ingress queue is full.

1. FCS = frame check sequence
2. MTU = maximum transmission unit

This is an example of output from the **show controllers ethernet-controller phy** command for a specific interface. Note that the last line of the display is the setting for automatic media-dependent-interface crossover (Auto-MDIX) for the interface.

```
Switch# show controllers ethernet-controller gigabitethernet1/0/3 phy

 Control Register                    :  0001 0001 0100 0000
 Control STATUS                      :  0111 1001 0100 1001
 Phy ID 1                            :  0000 0001 0100 0001
 Phy ID 2                            :  0000 1100 0010 0100
 Auto-Negotiation Advertisement      :  0000 0011 1110 0001
 Auto-Negotiation Link Partner       :  0000 0000 0000 0000
 Auto-Negotiation Expansion Reg      :  0000 0000 0000 0100
 Next Page Transmit Register         :  0010 0000 0000 0001
 Link Partner Next page Registe      :  0000 0000 0000 0000
 1000BASE-T Control Register         :  0000 1111 0000 0000
 1000BASE-T Status Register          :  0100 0000 0000 0000
 Extended Status Register            :  0011 0000 0000 0000
 PHY Specific Control Register       :  0000 0000 0111 1000
 PHY Specific Status Register        :  1000 0001 0100 0000
 Interrupt Enable                    :  0000 0000 0000 0000
 Interrupt Status                    :  0000 0000 0100 0000
 Extended PHY Specific Control       :  0000 1100 0110 1000
 Receive Error Counter               :  0000 0000 0000 0000
 Reserved Register 1                 :  0000 0000 0000 0000
 Global Status                       :  0000 0000 0000 0000
 LED Control                         :  0100 0001 0000 0000
 Manual LED Override                 :  0000 1000 0010 1010
 Extended PHY Specific Control       :  0000 0000 0001 1010
 Disable Receiver 1                  :  0000 0000 0000 1011
 Disable Receiver 2                  :  1000 0000 0000 0100
 Extended PHY Specific Status        :  1000 0100 1000 0000
 Auto-MDIX                           :  On   [AdminState=1   Flags=0x00052248]
```

This is an example of output from the **show controllers ethernet-controller port-asic configuration** command:

```
Switch# show controllers ethernet-controller port-asic configuration

================================================================================
Switch 4, PortASIC 0 Registers
--------------------------------------------------------------------------------
DeviceType                        : 000101BC
Reset                             : 00000000
PmadMicConfig                     : 00000001
PmadMicDiag                       : 00000003
SupervisorReceiveFifoSramInfo     : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo    : 000001D0 000001D0 40000000
GlobalStatus                      : 00000800
IndicationStatus                  : 00000000
```

```
IndicationStatusMask               : FFFFFFFF
InterruptStatus                    : 00000000
InterruptStatusMask                : 01FFE800
SupervisorDiag                     : 00000000
SupervisorFrameSizeLimit           : 000007C8
SupervisorBroadcast                : 000A0F01
GeneralIO                          : 000003F9 00000000 00000004
StackPcsInfo                       : FFFF1000 860329BD 5555FFFF FFFFFFFF
                                     FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo                       : 73001630 00000003 7F001644 00000003
                                     24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus                 : 18E418E0
stackControlStatusMask             : FFFFFFFF
TransmitBufferFreeListInfo         : 00000854 00000800 00000FF8 00000000
                                     0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo               : 00000016 00000016 40000000 00000000
                                     0000000C 0000000C 40000000 00000000
TransmitBufferInfo                 : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount          : 00000F7A
TransmitBufferCommonCountPeak      : 0000001E
TransmitBufferCommonCommonEmpty    : 000000FF
NetworkActivity                    : 00000000 00000000 00000000 02400000
DroppedStatistics                  : 00000000
FrameLengthDeltaSelect             : 00000001
SneakPortFifoInfo                  : 00000000
MacInfo                            : 0EC0801C 00000001 0EC0801B 00000001
                                     00C0001D 00000001 00C0001E 00000001

<output truncated>
```

This is an example of output from the **show controllers ethernet-controller port-asic statistics** command:

```
Switch# show controllers ethernet-controller port-asic statistics
==========================================================================
 Switch 1, PortASIC 0 Statistics
--------------------------------------------------------------------------
         0 RxQ-0, wt-0 enqueue frames           0 RxQ-0, wt-0 drop frames
   4118966 RxQ-0, wt-1 enqueue frames           0 RxQ-0, wt-1 drop frames
         0 RxQ-0, wt-2 enqueue frames           0 RxQ-0, wt-2 drop frames

         0 RxQ-1, wt-0 enqueue frames           0 RxQ-1, wt-0 drop frames
       296 RxQ-1, wt-1 enqueue frames           0 RxQ-1, wt-1 drop frames
   2836036 RxQ-1, wt-2 enqueue frames           0 RxQ-1, wt-2 drop frames

         0 RxQ-2, wt-0 enqueue frames           0 RxQ-2, wt-0 drop frames
         0 RxQ-2, wt-1 enqueue frames           0 RxQ-2, wt-1 drop frames
    158377 RxQ-2, wt-2 enqueue frames           0 RxQ-2, wt-2 drop frames

         0 RxQ-3, wt-0 enqueue frames           0 RxQ-3, wt-0 drop frames
         0 RxQ-3, wt-1 enqueue frames           0 RxQ-3, wt-1 drop frames
         0 RxQ-3, wt-2 enqueue frames           0 RxQ-3, wt-2 drop frames


        15 TxBufferFull Drop Count              0 Rx Fcs Error Frames
         0 TxBufferFrameDesc BadCrc16           0 Rx Invalid Oversize Frames
         0 TxBuffer Bandwidth Drop Cou          0 Rx Invalid Too Large Frames
         0 TxQueue Bandwidth Drop Coun          0 Rx Invalid Too Large Frames
         0 TxQueue Missed Drop Statist          0 Rx Invalid Too Small Frames
        74 RxBuffer Drop DestIndex Cou          0 Rx Too Old Frames
         0 SneakQueue Drop Count                0 Tx Too Old Frames
         0 Learning Queue Overflow Fra          0 System Fcs Error Frames
         0 Learning Cam Skip Count
```

```
         15 Sup Queue 0 Drop Frames                0 Sup Queue 8 Drop Frames
          0 Sup Queue 1 Drop Frames                0 Sup Queue 9 Drop Frames
          0 Sup Queue 2 Drop Frames                0 Sup Queue 10 Drop Frames
          0 Sup Queue 3 Drop Frames                0 Sup Queue 11 Drop Frames
          0 Sup Queue 4 Drop Frames                0 Sup Queue 12 Drop Frames
          0 Sup Queue 5 Drop Frames                0 Sup Queue 13 Drop Frames
          0 Sup Queue 6 Drop Frames                0 Sup Queue 14 Drop Frames
          0 Sup Queue 7 Drop Frames                0 Sup Queue 15 Drop Frames
=============================================================================
 Switch 1, PortASIC 1 Statistics
-----------------------------------------------------------------------------
          0 RxQ-0, wt-0 enqueue frames            0 RxQ-0, wt-0 drop frames
         52 RxQ-0, wt-1 enqueue frames            0 RxQ-0, wt-1 drop frames
          0 RxQ-0, wt-2 enqueue frames            0 RxQ-0, wt-2 drop frames

<output truncated>
```

Related Commands

Command	Description
show boot	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
show controllers tcam	Displays the state of registers for all ternary content addressable memory (TCAM) and TCAM ASICs.

show controllers tcam

Use the **show controllers tcam** privileged EXEC command to display the state of the registers for all ternary content addressable memory (TCAM) in the system and for all TCAM interface application-specific integrated circuits (ASICs) that are CAM controllers.

show controllers tcam [**asic** [**number**]] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

asic	(Optional) Display port ASIC TCAM information.
number	(Optional) Display information for the specified port ASIC number. The range is from 0 to 15.
detail	(Optional) Display detailed TCAM register information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **asic** [**number**] keywords were added.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

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

Examples

This is an example of output from the **show controllers tcam** command:

```
Switch# show controllers tcam

---------------------------------------------------------------------------
TCAM-0 Registers
---------------------------------------------------------------------------
  REV:    00B30103
  SIZE:   00080040
  ID:     00000000
  CCR:    00000000_F0000020

  RPID0:  00000000_00000000
  RPID1:  00000000_00000000
  RPID2:  00000000_00000000
  RPID3:  00000000_00000000

  HRR0:   00000000_E000CAFC
  HRR1:   00000000_00000000
  HRR2:   00000000_00000000
  HRR3:   00000000_00000000
  HRR4:   00000000_00000000
  HRR5:   00000000_00000000
  HRR6:   00000000_00000000
  HRR7:   00000000_00000000
<output truncated>

  GMR31:  FF_FFFFFFFF_FFFFFFFF
  GMR32:  FF_FFFFFFFF_FFFFFFFF
  GMR33:  FF_FFFFFFFF_FFFFFFFF

===========================================================================
 TCAM related PortASIC 1 registers
===========================================================================
LookupType:                   89A1C67D_24E35F00
LastCamIndex:                 0000FFE0
LocalNoMatch:                 000069E0
ForwardingRamBaseAddress:
                              00022A00 0002FE00 00040600 0002FE00 0000D400
                              00000000 003FBA00 00009000 00009000 00040600
                              00000000 00012800 00012900
```

Related Commands

Command	Description
show controllers cpu-interface	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.

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 *interface-id*	(Optional) Display the 802.1X status for the specified interface (including type, stack member, module, and port number).
statistics interface *interface-id*	(Optional) Display 802.1X statistics for the specified interface (including type, stack member, module, and port number).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	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 are displayed. If you specify an interface, details for that interface are displayed.

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

Examples

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 GigabitEthernet1/0/3
----------------------------------------------------
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 GigabitEthernet1/0/7
----------------------------------------------------
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 gigabitethernet1/0/3** privileged EXEC command:

```
Switch# show dot1x interface gigabitethernet1/0/3
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 gigabitethernet1/0/3** command. Table 2-20 describes the fields in the display.

```
Switch# show dot1x statistics interface gigabitethernet1/0/3
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 2-20 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.
RxLenError	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	Number of 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 dtp

Use the **show dtp** privileged EXEC command to display Dynamic Trunking Protocol (DTP) information for the switch or for a specified interface.

show dtp [**interface** *interface-id*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, stack member, module, and port number).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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

```
Switch# show dtp
Global DTP information
        Sending DTP Hello packets every 30 seconds
        Dynamic Trunk timeout is 300 seconds
        21 interfaces using DTP
```

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

```
Switch# show dtp interface gigabitethernet1/0/1
DTP information for GigabitEthernet1/0/1:
  TOS/TAS/TNS:                              ACCESS/AUTO/ACCESS
  TOT/TAT/TNT:                              NATIVE/NEGOTIATE/NATIVE
  Neighbor address 1:                       000943A7D081
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       1/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S2:ACCESS
  # times multi & trunk                     0
  Enabled:                                  yes
  In STP:                                   no

  Statistics
  ----------
  3160 packets received (3160 good)
  0 packets dropped
      0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
  6320 packets output (6320 good)
      3160 native, 3160 software encap isl, 0 isl hardware native
  0 output errors
  0 trunk timeouts
  1 link ups, last link up on Mon Mar 01 1993, 01:02:29
  0 link downs
```

Related Commands

Command	Description
show interfaces trunk	Displays interface trunking information.

show env

Use the **show env** user EXEC command to display fan, temperature, redundant power system (RPS) availability, and power information for the switch being accessed (standalone switch or stack master or stack member). Use with the **stack** keyword to display all information for the stack or for a specified switch in the stack.

show env {**all** | **fan** | **power** | **rps** | **stack** [*switch-number*] | **temperature**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display both fan and temperature environmental status.
fan	Display the switch fan status.
power	Display the switch power status.
rps	Display whether an RPS 300 Redundant Power System is connected to the switch.
stack [*switch-number*]	Display all environmental status for each switch in the stack or for the specified switch. The range is 1 to 9, depending on the switch member numbers in the stack.
temperature	Display the switch temperature status.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

Use the show access-lists privileged EXEC command to access information from a specific switch other than the master.

You can use the **show env stack** [*switch-number*] command to display information about any switch in the stack from any switch member.

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

Examples

This is an example of output from the **show env all** command entered from the master switch or a standalone switch:

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is AVAILABLE
```

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

```
Switch> show env fan
FAN is OK
```

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

```
Switch> show env stack
SWITCH: 1
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 2
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 4
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 5
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 6
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

This example shows how to display information about stack member 3 from the master switch:

```
Switch> show env stack 3
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

show errdisable detect

Use the **show errdisable detect** user EXEC command to display error-disable detection status.

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

A displayed gbic-invalid error reason refers to an invalid small form-factor pluggable (SFP) module.

Examples

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

```
Switch> show errdisable detect
ErrDisable Reason    Detection status
-----------------    ----------------
udld                 Enabled
bpduguard            Enabled
security-violation   Enabled
channel-misconfig    Enabled
psecure-violation    Enabled
dhcp-rate-limit      Enabled
unicast-flood        Enabled
vmps                 Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
gbic-invalid         Enabled
loopback             Enabled
```

Note Though visible in the output, the dhcp-rate-limit and unicast-flood fields are not valid.

Related Commands

Command	Description
errdisable detect cause	Enables error-disable detection for a specific cause or all causes.
show errdisable flap-values	Displays error condition recognition information.
show errdisable recovery	Displays error-disable recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show errdisable flap-values

Use the **show errdisable flap-values** user EXEC command to display conditions that cause an error to be recognized for a cause.

show errdisable flap-values [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

The *Flaps* column in the display shows how many changes to the state within the specified time interval will cause an error to be detected and a port to be disabled. For example, the display shows that an error will be assumed and the port shut down if three Dynamic Trunking Protocol (DTP)-state (port mode access/trunk) or Port Aggregation Protocol (PAgP) flap changes occur during a 30-second interval, or if 5 link-state (link up/down) changes occur during a 10-second interval.

```
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

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

Examples

This is an example of output from the **show errdisable flap-values** command:

```
Switch> show errdisable flap-values
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disable detection for a specific cause or all causes.
show errdisable detect	Displays error-disable detection status.
show errdisable recovery	Displays error-disable recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

A gbic-invalid error-disable reason refers to an invalid small form-factor pluggable (SFP) interface.

Examples

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

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
gbic-invalid         Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
loopback             Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi1/0/4           link-flap             279
```

Related Commands

Command	Description
errdisable recovery	Configures the recover mechanism variables.
show errdisable detect	Displays error disable detection status.
show errdisable flap-values	Displays error condition recognition information.
show interfaces status	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** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 12.
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.
protocol	Display the protocol that is being used in the EtherChannel.
summary	Display a one-line summary per channel-group.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **protocol** keyword was added.

Usage Guidelines

If you do not specify a *channel-group*, all channel groups are displayed.

In the output, the Passive port list field is displayed only for Layer 3 port channels. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly is in the only port channel in the channel group).

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

Examples

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

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
               Ports in the group:
               -------------------
Port: Gi1/0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   =   -         Pseudo port-channel = Po1
Port index    = 0           Load = 0x00        Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Gi1/0/1   SA      bndl      32768         0x1       0x1     0x101    0x3D
Gi1/0/2   SA      bndl      32768         0x0       0x1     0x0      0x3D
Gi0/1     SA      bndl      32768         0x0       0x1     0x0      0x3D

Age of the port in the current state: 01d:20h:06m:04s

               Port-channels in the group:
               ----------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 01d:20h:20m:26s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/1  Active          0
  0     00     Gi1/0/2  Active          0
  0     00     Gi0/1    Active            0
  0     00     Gi0/2    Active            0

Time since last port bundled:    01d:20h:20m:20s    Gi1/0/2
```

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
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         LACP      Gi1/0/1(P)  Gi1/0/2(P)
1      Po1(SU)         LACP      Gi0/1(P)     Gi0/2(P)
```

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

```
Switch> show etherchannel 1 port-channel
                Port-channels in the group:
                ----------------------
Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 01d:20h:24m:50s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/1  Active    0
  0     00     Gi1/0/2  Active    0
  0     00     Gi0/1    Active    0
  0     00     Gi0/2    Active    0

Time since last port bundled:    01d:20h:24m:44s    Gi1/0/2
```

This is an example of output from **show etherchannel protocol** command:

```
Switch# show etherchannel protocol
                Channel-group listing:
                ----------------------
Group: 1
----------
Protocol:  LACP

Group: 2
----------
Protocol:  PAgP
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet interface to an EtherChannel group.

Command	Description
channel-protocol	Restricts the protocol used on an interface to manage channeling.
interface port-channel	Accesses or creates the port channel.

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** *number*] | **counters** | **description** | **etherchannel** | **flowcontrol** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Valid interfaces include physical ports (including type, stack member, module, and port number) and port channels. The valid port-channel range is 1 to 12.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Display accounting information on the interface, including active protocols and input and output packets and octets.
capabilities	(Optional) Display the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module *number*	(Optional) Display capabilities of all interfaces on the specified stack member switch. The range is from 1 to 9. Although the indicated range is from 1 to 9, entering only module 1 displays the switch capabilities. This option is not available if you enter a specific interface ID before the **capabilities** keyword.
counters	(Optional) See the **show interfaces counters** command.
description	(Optional) Display the administrative status and description set for an interface.
etherchannel	(Optional) Display interface EtherChannel information.
flowcontrol	(Optional) Display interface flowcontrol information
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, including port blocking and port protection settings.
trunk	Display interface trunk information. If you do not specify an interface, information for only active trunking ports is displayed.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	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**, **private-vlan mapping**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	Support for the **capabilities** keyword was added.

Usage Guidelines The **show interfaces capabilities** command with different keywords has these results:

- Entering **show interface capabilities module** *number* displays the capabilities of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, the output is blank. **1** displays the capabilities of all interfaces on the switch. If you enter any other number, the output is blank.
- Entering **show interfaces** *interface-id* **capabilities** displays the capabilities of the specified interface.
- Entering **show interfaces capabilities** (with no module number or interface ID) displays the capabilities of all interfaces on the switch in the stack.

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

Examples This is an example of output from the **show interfaces** command for Gigabit Ethernet interface 3 on stack member 3:

```
Switch# show interfaces gigabitethernet3/0/3
GigabitEthernet3/0/3 is down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)
  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
  ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, 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
     2 packets input, 1040 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
     4 packets output, 1040 bytes, 0 underruns
     0 output errors, 0 collisions, 3 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 accounting** command.

```
Switch# show interfaces accounting
Vlan1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP    1094395  131900022     559555   84077157
           Spanning Tree     283896   17033760         42       2520
                     ARP      63738    3825680        231      13860
Interface Vlan2 is disabled
Vlan7
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Vlan31
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.

GigabitEthernet1/0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/3
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.

<output truncated>
```

This is an example of output from the **show interfaces capabilities** command for an interface.

```
Switch# show interfaces gigabitethernet1/0/3 capabilities
GigabitEthernet1/0/3
  Model:                 WS-C3750G-24TS
  Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                full,auto
  Trunk encap. type:     802.1Q,ISL
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on,desired),tx-(none)
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),tx-(4q2t)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
  Inline power:          no
  SPAN:                  source/destination
  PortSecure:            yes
  Dot1x:                 yes
  Dot1x:                 yes

Switch# show interfaces gigabitethernet0/1 capabilities
GigabitEthernet0/1
  Model:                 WS-C2970G-24T-E
  Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                full,auto
  Trunk encap. type:     802.1Q,ISL
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on,desired),tx-(none)
  Fast Start:            yes
```

```
QoS scheduling:         rx-(not configurable on per port basis),tx-(4q2t)
CoS rewrite:            yes
ToS rewrite:            yes
UDLD:                   yes
Inline power:           no
SPAN:                   source/destination
PortSecure:             yes
Dot1x:                  yes
```

This is an example of output from the **show interfaces gigabitethernet1/0/4 description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```
Switch# show interfaces gigabitethernet1/0/4 description
Interface Status         Protocol Description
Gi1/0/4     up             down     Connects to Marketing
Gi0/4       up             down     Connects to Marketing
```

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

```
Switch# show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/2          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/3          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 interfaces gigabitethernet1/0/6 pruning** command when pruning is enabled in the VTP domain:

```
Switch# show interfaces gigibitethernet1/0/6 pruning
Port    Vlans pruned for lack of request by neighbor
Gi1/0/6   3,4
Gi0/6     3,4

Port    Vlans traffic requested of neighbor
Gi1/0/6   1-3
Gi0/6     1-3
```

This is an example of output from the **show interfaces stats** command for a specified interface.

```
Switch# show interfaces vlan 1 stats
Switching path    Pkts In   Chars In   Pkts Out  Chars Out
        Processor    1165354  136205310     570800   91731594
      Route cache          0          0          0          0
            Total    1165354  136205310     570800   91731594
```

This is an example of partial 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
Fa1/0/1                      notconnect   1            auto   auto 10/100BaseTX
Fa1/0/2                      notconnect   1            auto   auto 10/100BaseTX
Fa1/0/3                      notconnect   1            auto   auto 10/100BaseTX
Fa1/0/4   Test               notconnect   1            auto   auto 10/100BaseTX
Fa1/0/5                      notconnect   1            auto   auto 10/100BaseTX
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/1                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/2                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/3                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/4                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/5                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/6                        notconnect   1            auto   auto 10/100/1000BaseTX

<output truncated>
```

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

```
Switch# show interfaces status err-disabled
Port      Name               Status       Reason
Gi2/0/26                     err-disabled gbic-invalid
Gi0/6                        err-disabled dtp-flap
```

This is an example of output from the **show interfaces switchport** command for a single interface. Table 2-21 describes the fields in the display.

Note Private VLANs are not supported in this release, so those fields are not applicable.

```
Switch# show interfaces gigabitethernet1/0/3 switchport
Name: Gi1/0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
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
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Appliance trust: none
```

Table 2-21 show interfaces switchport Field Descriptions

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational modes.
Administrative Trunking Encapsulation Operational 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.

Table 2-21 show interfaces switchport Field Descriptions (continued)

Field	Description
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.
Protected	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.
Appliance trust	Displays the CoS setting of the data packets of the IP phone.

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

```
Switch# show interfaces fastethernet1/0/17 trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa1/0/17    desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Fa1/0/17    1-4094

Port        Vlans allowed and active in management domain
Fa1/0/17    1-4,20,34-36,38-55,57-58,66-67,100,139,200-201,1000

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/17    1-4,20,34-36,38-55,57-58,66-67,100,139,200-201,1000
e
Switch# show interfaces gigabitethernet0/1 trunk
Port        Mode         Encapsulation  Status        Native vlan
Gi0/1       auto         negotiate      trunking      1

Port        Vlans allowed on trunk
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1-4

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1-4
```

Related Commands

Command	Description
switchport access	Configures a port as a static-access or dynamic-access port.
switchport block	Blocks unknown unicast or multicast traffic on an interface.
switchport mode	Configures the VLAN membership mode of a port.
switchport protected	Isolates unicast, multicast, and broadcast traffic at Layer 2 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 the switch or for a specific interface.

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

Syntax Descriptions

interface-id	(Optional) ID of the physical interface, including type, stack member, module, and port number.
vlan *vlan-id*	(Optional) VLAN number of the management VLAN. The range is 1 to 4094.
broadcast	(Optional) Display discarded broadcast traffic.
errors	(Optional) Display error counters.
module *switch- number*	(Optional) Display counters for the specified stack member. The range is from 1 to 9, depending upon the switch numbers in the stack. **Note** In this command, the **module** keyword refers to the stack member number (1–9). In other commands that contain an interface ID, the **module** number is always zero.
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 *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	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* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Switch# show interfaces counters
Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Fa6/0/1                0             0             0             0
Fa6/0/2                0             0             0             0
Fa6/0/3                0             0             0             0
Fa6/0/4                0             0             0             0
Fa6/0/5                0             0             0             0

<output truncated>

Fa6/0/24               0             0             0             0
Gi6/0/1                0             0             0             0
Gi6/0/2                0             0             0             0
Fa8/0/1                0             0             0             0
Fa8/0/2                0             0             0             0

Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi0/1                  0             0             0             0
Gi0/2                  0             0             0             0
Gi0/3                  0             0             0             0
Gi0/4                  0             0             0             0
Gi0/5                  0             0             0             0
Gi0/6                  0             0             0             0
Gi0/7                  0             0             0             0
Gi0/8                  0             0             0             0
Gi0/9                  0             0             0             0

<output truncated>
```

This is an example of partial output from the **show interfaces counters broadcast** command. It displays dropped broadcast traffic for all interfaces.

```
Switch# show interfaces counters broadcast

Port      BcastSuppDiscards
Fa1/0/1                   0
Fa1/0/2                   0
Fa1/0/3                   0
Fa1/0/4                   0
Fa1/0/5                   0
Fa1/0/6                   0

Gi0/1                     0
Gi0/2                     0
Gi0/3                     0
Gi0/4                     0
Gi0/5                     0
Gi0/6                     0

<output truncated>
```

This is an example of partial output from the **show interfaces counters module** command for stack member 2. It displays all counters for the specified switch in the stack.

```
Switch# show interfaces counters module 2
Sauron#show interface counters

Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Fa2/0/1              520             2             0             0
Fa2/0/2              520             2             0             0
Fa2/0/3              520             2             0             0
```

```
Fa2/0/4             520             2               0               0
Fa2/0/5             520             2               0               0
Fa2/0/6             520             2               0               0
Fa2/0/7             520             2               0               0
Fa2/0/8             520             2               0               0

<output truncated>
```

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

```
Switch# show interfaces counters trunk

Port        TrunkFramesTx  TrunkFramesRx  WrongEncap
Fa1/0/1                 0              0           0
Fa1/0/2                 0              0           0
Fa1/0/3             80678           4155           0
Fa1/0/4             82320            126           0
Fa1/0/5                 0              0           0

Gi0/1                   0              0           0
Gi0/2                   0              0           0
Gi0/3               80678           4155           0
Gi0/4               82320            126           0
Gi0/5                   0              0           0

<output truncated>
```

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.
show storm-control	Displays storm-control settings for an interface or all interfaces.
storm-control	Sets storm-control broadcast, multicast, and unicast suppression levels for an interface.

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

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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.

show ip igmp snooping [**group** | **mrouter** | **multicast** | **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 assoicated with each group.
mrouter	(Optional) See the **show ip igmp snooping mrouter** command.
multicast	(Optional) See the **show ip igmp snooping multicast** command.
querier	(Optional) Display information about the IGMP version that an interface supports.
vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **group** and **querier** keywords were added.

Usage Guidelines

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

Although visible in the output display, output lines related to topology change notification (TCN) and source-only learning are not supported.

Use the **show ip igmp snooping group** command to display the multicast groups, the compatibility mode, and the ports that are assoicated with each group.

Use the **show ip igmp snooping querier** command 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* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN.

```
Switch> show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             :Enabled
IGMPv3 snooping support   :Basic
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
```

Note TCN and source-only learning are not supported, and information displayed about these features is not valid.

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
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 group vlan 1** command:

```
Switch> show ip igmp snooping group vlan 1

Vlan      Group           Version     Port List
------------------------------------------------------------
1         229.2.3.4       v3          gi1/0/1 gi1/0/3
1         224.1.1.1       v2          gi1/0/8
```

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                  gi1/0/1
2         172.20.40.20    v2                  Router
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or on a VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN
show ip igmp snooping multicast	Displays IGMP snooping multicast information for the switch or for the specified parameter.

show ip igmp snooping mrouter

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

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

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12/1(11)AX	This command was first introduced.

Usage Guidelines

Use this command to display multicast router ports on the switch or for a specific VLAN.

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

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

Examples

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the switch.

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or on a VLAN.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN
show ip igmp snooping multicast	Displays IGMP snooping multicast information for the switch or for the specified parameter.

show ip igmp snooping multicast

Use the **show ip igmp snooping multicast** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping multicast table for the switch or multicast information for the selected parameter. Use with the **vlan** keyword to display the multicast table for a specified multicast VLAN or information about the selected parameter for the VLAN.

show ip igmp snooping multicast [**vlan** *vlan-id*] [**count** | **dynamic** [**count** | **group** *ip_address*] | **group** *ip_address* | **user** [**count** | **group** *ip_address*]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 4094.
count	(Optional) Display the total number of entries for the specified command options instead of the actual entries.
dynamic	(Optional) Display entries learned through IGMP snooping.
group *ip_address*	(Optional) Display characteristics of the multicast group with the specified group IP address.
user	(Optional) Display only the user-configured multicast entries.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

Use this command to display multicast information and the multicast table for specified parameters.

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

Examples

This is an example of output from the **show ip igmp snooping multicast** command without any keywords. It displays the multicast table for the switch.

```
Switch# show ip igmp snooping multicast

Vlan    Group Address     Type       Ports
----    -------------     ----       -----
   1    224.1.2.30        IGMP       Fa3/0/31, Fa4/0/1 Gi0/3, Gi0/4
   1    224.1.2.1         IGMP       Fa3/0/31, Fa4/0/1 Gi0/3, Gi0/4
   1    224.4.4.4         USER       Fa1/0/4, Fa4/0/1 Gi0/10, Gi0/11
```

This is an example of output from the **show ip igmp snooping multicast count** command. It displays the total number of multicast groups on the switch.

```
Switch# show ip igmp snooping multicast count
Total number of multicast groups: 3
```

This is an example of output from the **show ip igmp snooping multicast dynamic** command. It shows only the entries learned through IGMP snooping.

```
Switch# show ip igmp snooping multicast dynamic

Vlan    Group Address     Type       Ports
----    -------------     ----       -----
   1    224.1.2.30        IGMP       Fa4/0/1, Fa4/0/37 Gi0/3, Gi0/4
   1    224.1.2.1         IGMP       Fa4/0/1, Fa4/0/37 Gi0/3, Gi0/4
```

This is an example of output from the **show ip igmp snooping multicast group** command. It shows the entries for the group with the specified IP address.

```
Switch# show ip igmp snooping multicast group 224.1.2.30
Vlan    Group Address     Type       Ports
----    -------------     ----       -----
   1    224.1.2.30        IGMP       Fa4/0/1, Fa4/0/37 Gi0/3, Gi0/4
```

This is an example of output from the **show ip igmp snooping multicast vlan** command. It displays all entries belonging to the specified VLAN.

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

Vlan    Group Address     Type       Ports
----    -------------     ----       -----
   1    224.1.2.30        IGMP       Fa4/0/1, Fa4/0/37 Gi0/3, Gi0/4
   1    224.1.2.1         IGMP       Fa4/0/1, Fa4/0/37 Gi0/3, Gi0/4
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or on a VLAN.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast 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** | **sys-id**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 12.
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 the switch MAC address.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

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

Usage Guidelines

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

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* option to specify a channel group for all keywords except **sys-id**.

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 user EXEC command. Table 2-22 describes the fields in the display.

```
Switch> show lacp counters
               LACPDUs          Marker      Marker Response    LACPDUs
Port          Sent    Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group:1
Gi2/0/5       19      10       0      0        0      0         0
Gi2/0/6       14      6        0      0        0      0         0
Gi2/0/7       8       7        0      0        0      0         0
```

Table 2-22 show lacp counters Field Descriptions

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by an interface.
Marker Sent and Recv	The number of LACP marker packets sent and received by an interface.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by an interface.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for an interface.

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

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port     Port
Port        Flags   State   Priority      Key       Key     Number   State
Gi2/0/5     SA      bndl    32768         0x3       0x3     0x4      0x3D
Gi2/0/6     SA      bndl    32768         0x3       0x3     0x5      0x3D
Gi2/0/7     SA      bndl    32768         0x3       0x3     0x6      0x3D
```

Table 2-23 describes the fields in the display:

Table 2-23 show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: • – —Port is in an unknown state. • **bndl**—Port is attached to an aggregator and bundled with other ports. • **susp**—Port is in a suspended state; it is not attached to any aggregator. • **hot-sby**—Port is in a hot-standby state. • **indiv**—Port is incapable of bundling with any other port. • **indep**—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). • **down**—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports s in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port number.
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired

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 3 neighbors

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi2/0/3   32768,0007.eb49.5e80  0xC               19s       SP

          LACP Partner         Partner         Partner
          Port Priority        Oper Key        Port State
          32768                0x3             0x3C

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi2/0/4   32768,0007.eb49.5e80  0xD               15s       SP

          LACP Partner         Partner         Partner
          Port Priority        Oper Key        Port State
          32768                0x3             0x3C
```

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

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

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

Related Commands

Command	Description
clear lacp	Clears LACP channel-group information.
lacp port-priority	Configures the LACP port priority.
lacp system-priority	Configures the LACP system priority.

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*]

Syntax Description

interface *interface-id*	(Optional) Display the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port channel range is 1 to 64.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC; the **interface** keyword is available only in privileged EXEC mode.

Command History

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

Usage Guidelines

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

Examples

This is an example of output from the **show mac-access group** user EXEC command. In this display, Gigabit Ethernet interface 1/0/12 has the MAC access list *macl_e1* applied; no MAC ACLs are applied to other interfaces.

```
Switch> show mac access-group
Interface GigabitEthernet1/0/1:
   Inbound access-list is not set
Interface GigabitEthernet1/0/2:
   Inbound access-list is macl_e1
Interface GigabitEthernet1/0/3:
   Inbound access-list is not set
Interface GigabitEthernet1/0/4:
   Inbound access-list is not set

<output truncated>

Interface GigabitEthernet1/0/10:
   Inbound access-list is not set
Interface GigabitEthernet1/0/11:
Inbound access-list is not set
Interface GigabitEthernet1/0/12:
   Inbound access-list is macl_e1

<output truncated>
```

This is an example of output from the **show mac access-group interface gigabitethernet1/ 0/12** command:

```
Switch# show mac access-group interface gigabitethernet1/0/12
Interface GigabitEthernet1/0/12:
   Inbound access-list is macl_e1
```

Related Commands

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

show mac address-table

Use the **show mac address-table** user EXEC command to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN.

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table** command replaces the **show mac-address-table** command (with the hyphen). The **show mac-address-table** command (with the hyphen) will become obsolete in a future release.

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **show mac-address-table** command was replaced by the **show mac address-table** command.

Usage Guidelines

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

Examples

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

```
Switch> show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
 All    0000.0000.0001    STATIC     CPU
 All    0000.0000.0002    STATIC     CPU
 All    0000.0000.0003    STATIC     CPU
 All    0000.0000.0009    STATIC     CPU
 All    0000.0000.0012    STATIC     CPU
 All    0180.c200.000b    STATIC     CPU
 All    0180.c200.000c    STATIC     CPU
 All    0180.c200.000d    STATIC     CPU
 All    0180.c200.000e    STATIC     CPU
 All    0180.c200.000f    STATIC     CPU
```

```
 All    0180.c200.0010    STATIC     CPU
   1    0030.9441.6327    DYNAMIC    Gi6/0/23
Total Mac Addresses for this criterion: 12
```

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 aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table address

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

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table address** command replaces the **show mac-address-table address** command (with the hyphen). The **show mac-address-table address** command (with the hyphen) will become obsolete in a future release.

Syntax Description

mac-address	Specify the 48-bit MAC address; the valid format is H.H.H.
interface *interface-id*	(Optional) Display information for a specific interface. Valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for the specific VLAN only. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **show mac-address-table address** command was replaced by the **show mac address-table address** command.

Usage Guidelines

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

Examples

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

```
Switch# show mac address-table address 0002.4b28.c482
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0002.4b28.c482  STATIC  CPU
Total Mac Addresses for this criterion: 1
```

Related Commands

Command	Description
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table aging-time

Use the **show mac address-table aging-time** user EXEC command to display the aging time of a specific address table instance, all address table instances on a specified VLAN or, if a specific VLAN is not specified, on all VLANs.

show mac address-table aging-time [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table aging-time** command replaces the **show mac-address-table aging-time** command (with the hyphen). The **show mac-address-table aging-time** command (with the hyphen) will become obsolete in a future release.

Syntax Description

vlan *vlan-id*	(Optional) Display aging time information for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **show mac-address-table aging-time** command was replaced by the **show mac address-table aging-time** command.

Usage Guidelines

If no VLAN number is specified, then the aging time for all VLANs is displayed.

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

Examples

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     300
```

This is an example of output from the **show mac address-table aging-time vlan 10** command:

```
Switch> show mac address-table aging-time vlan 10
Vlan    Aging Time
----    ----------
  10     300
```

Related Commands

Command	Description
mac address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table count

Use the **show mac address-table count** user EXEC command to display the number of addresses present in all VLANs or the specified VLAN.

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table count** command replaces the **show mac-address-table count** command (with the hyphen). The **show mac-address-table count** command (with the hyphen) will become obsolete in a future release.

Syntax Description

vlan *vlan-id*	(Optional) Display the number of addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **show mac-address-table count** command was replaced by the **show mac address-table count** command.

Usage Guidelines

If no VLAN number is specified, the address count for all VLANs is displayed.

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

Examples

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

```
Switch# show mac address-table count

Mac Entries for Vlan   : 1
---------------------------
Dynamic Address Count  : 2
Static  Address Count  : 0
Total Mac Addresses    : 2
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table dynamic

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

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table dynamic** command replaces the **show mac-address-table dynamic** command (with the hyphen). The **show mac-address-table dynamic** command (with the hyphen) will become obsolete in a future release.

Syntax Description

address *mac-address*	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
interface *interface-id*	(Optional) Specify an interface to match; valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC; **address** keyword available only in privileged EXEC mode.

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **show mac-address-table dynamic** command was replaced by the **show mac address-table dynamic** command.

Usage Guidelines

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

Examples

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

```
Switch> show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi6/0/2
   1    00b0.6496.2741  DYNAMIC Gi6/0/2
Total Mac Addresses for this criterion: 2
```

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 address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table interface

Use the **show mac address-table interface** user command to display the MAC address table information for the specified interface in the specified VLAN.

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table interface** command replaces the **show mac-address-table interface** command (with the hyphen). The **show mac-address-table interface** command (with the hyphen) will become obsolete in a future release.

Syntax Description

interface-id	Specify an interface type; valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **show mac-address-table interface** command was replaced by the **show mac address-table interface** command.

Usage Guidelines

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

Examples

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

```
Switch> show mac address-table interface gigabitethernet6/0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi6/0/2
   1    00b0.6496.2741  DYNAMIC Gi6/0/2
Total Mac Addresses for this criterion: 2
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table multicast

Use the **show mac address-table multicast** user EXEC command to display the Layer 2 multicast entries for all VLANs. Use the command in privileged EXEC mode to display specific multicast entries.

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table multicast** command replaces the **show mac-address-table multicast** command (with the hyphen). The **show mac-address-table multicast** command (with the hyphen) will become obsolete in a future release.

Syntax Description

vlan *vlan-id*	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
count	(Optional) Display the total number of entries for the specified command options instead of the actual entries.
user	(Optional) Display only the user-configured multicast entries.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **igmp-snooping** keyword is not supported. Use the **show ip igmp snooping multicast** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping multicast table.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)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* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show mac address-table multicast** command. It shows how to display all multicast entries for the switch.

```
Switch> show mac address-table multicast
Vlan    Mac Address      Type    Ports
----    -----------      ----    -----
   1    0100.5e00.0128   IGMP    Gi1/0/1
```

This is an example of output from the **show mac address-table multicast count** command. It shows how to display a total count of MAC address entries for the switch.

```
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. It shows how to display a total count of MAC address entries for a VLAN.

```
Switch> show mac address-table multicast vlan 1 count

Multicast MAC Entries for vlan 1:    4
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table notification

Use the **show mac address-table notification** user EXEC command to display the MAC address notification settings for all interfaces or the specified interface.

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table notification** command replaces the **show mac-address-table notification** command (with the hyphen). The **show mac-address-table notification** command (with the hyphen) will become obsolete in a future release.

Syntax Description

interface	(Optional) Display information for all interfaces. Valid interfaces include physical ports and port channels.
interface-id	(Optional) Display information for the specified interface. Valid interfaces include physical ports and port channels.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)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 any keywords to display whether the feature is enabled or disabled, the MAC notification interval, the maximum number of entries allowed in the history table, and the history table contents.

Use the **interface** keyword to display the flags for all interfaces. If the *interface-id* is included, only the flags for that interface are displayed.

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

Examples

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

```
Switch> show mac address-table notification
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
----------------------
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1
```

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table static

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

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table static** command replaces the **show mac-address-table static** command (with the hyphen). The **show mac-address-table static** command (with the hyphen) will become obsolete in a future release.

Syntax Description

address *mac-address*	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
interface *interface-id*	(Optional) Specify an interface to match; valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC; **address** keyword available only in privileged EXEC mode.

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **show mac-address-table static** command was replaced by the **show mac address-table static** command.

Usage Guidelines

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

Examples

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

```
Switch> show mac address-table static
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0100.0ccc.cccc  STATIC  CPU
 All    0180.c200.0000  STATIC  CPU
 All    0100.0ccc.cccd  STATIC  CPU
```

```
 All    0180.c200.0001  STATIC  CPU
 All    0180.c200.0002  STATIC  CPU
 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
Total Mac Addresses for this criterion: 10
```

Related Commands

Command	Description
mac address-table static	Adds static addresses to the MAC address table.
mac address-table static drop	Enables unicast MAC address filtering, and configures the switch to drop traffic with a specific source or destination MAC address.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table vlan

Use the **show mac address-table vlan** user EXEC command to display the MAC address table information for the specified VLAN.

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

Note Beginning with Cisco IOS Release 12.1(19)EA1, the **show mac address-table vlan** command replaces the **show mac-address-table vlan** command (with the hyphen). The **show mac-address-table vlan** command (with the hyphen) will become obsolete in a future release.

Syntax Description

vlan-id	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(19)EA1	The **show mac-address-table vlan** command was replaced by the **show mac address-table vlan** command.

Usage Guidelines

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

Examples

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

```
Switch> show mac address-table vlan 1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.0ccc.cccc  STATIC  CPU
   1    0180.c200.0000  STATIC  CPU
   1    0100.0ccc.cccd  STATIC  CPU
   1    0180.c200.0001  STATIC  CPU
   1    0180.c200.0002  STATIC  CPU
   1    0180.c200.0003  STATIC  CPU
   1    0180.c200.0004  STATIC  CPU
   1    0180.c200.0005  STATIC  CPU
   1    0180.c200.0006  STATIC  CPU
   1    0180.c200.0007  STATIC  CPU
```

```
Total Mac Addresses for this criterion: 10
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.

show mls qos

Use the **show mls qos** user EXEC command to display global quality of service (QoS) configuration information.

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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

```
Switch> show mls qos
Qos is enabled
```

Related Commands

Command	Description
mls qos	Enables quality of service (QoS) for the entire switch.

show mls qos aggregate-policer

Use the **show mls qos aggregate-policer** user EXEC command to display the quality of service (QoS) aggregate policer configuration. A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

show mls qos aggregate-policer [*aggregate-policer-name*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mls qos aggregate-policer** command:

```
Switch> show mls qos aggregate-policer policer1
aggregate-policer policer1 88000 2000000 exceed-action drop
Not used by any policy map
```

Related Commands

Command	Description
mls qos aggregate-policer	Defines policer parameters that can be shared by multiple classes within a policy map.

show mls qos input-queue

Use the **show mls qos input-queue** user EXEC command to display quality of service (QoS) settings for the ingress queues.

show mls qos input-queue [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mls qos input-queue** command:

```
Switch> show mls qos input-queue
Queue     :       1       2
-------------------------------------------
buffers   :       90      10
bandwidth :       4       4
priority  :       0       10
threshold1:       100     100
threshold2:       100     100
```

Related Commands

Command	Description
mls qos srr-queue input bandwidth	Assigns shaped round robin (SRR) weights to an ingress queue.
mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
mls qos srr-queue input cos-map	Maps assigned class of service (CoS) values to an ingress queue and assigns CoS values to a queue and to a threshold ID.
mls qos srr-queue input dscp-map	Maps assigned Differentiated Services Code Point (DSCP) values to an ingress queue and assigns DSCP values to a queue and to a threshold ID.
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue input threshold	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.

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*] [**buffers** | **queueing** | **statistics**]
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Display QoS information for the specified interface. Valid interfaces include physical ports.
buffers	(Optional) Display the buffer allocation among the queues.
queueing	(Optional) Display the queueing strategy (shared or shaped) and the weights corresponding to the queues.
statistics	(Optional) Display statistics for sent and received Differentiated Services Code Points (DSCPs) and class of service (CoS) values, the number of packets enqueued or dropped per egress queue, and the number of in-profile and out-of-profile packets for each policer.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **policers** keyword is not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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

```
Switch# show mls qos interface fastethernet1/0/7
FastEthernet1/0/7
Switch# show mls qos interface gigabitethernet0/7
GigabitEthernet0/7
Attached policy-map for Ingress: videowizard_policy
trust state: not trusted
COS override: dis
default COS: 0
```

```
DSCP Mutation Map: Default DSCP Mutation Map
```

This is an example of output from the **show mls qos interface fastethernet1/0/7 buffersshow mls qos interface gigabitethernet0/7 buffers** command:

```
Switch> show mls qos interface fastethernet1/0/7 buffers
Switch> show mls qos interface gigabitethernet0/7 buffers
FastEthernet1/0/7
GigabitEthernet0/7
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

This is an example of output from the **show mls qos interface fastethernet1/0/7 queueingshow mls qos interface gigabitethernet0/7 queueing** command. The egress expedite queue overrides the configured SRR weights.

```
Switch> show mls qos interface fastethernet1/0/7 queueing
Switch> show mls qos interface gigabitethernet0/7 queueing
FastEthernet1/0/7
Egress Priority Queue :enabled
GigabitEthernet0/7
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  25 25 25 25
The port bandwidth is limited to: 100%
The port is mapped to qset : 1
```

This is an example of output from the **show mls qos interface fastethernet1/0/7 statisticsshow mls qos interface gigabitethernet0/7 statistics** command. Table 2-24 describes the fields in this display.

```
Switch> show mls qos interface fastethernet1/0/7 statistics
Switch> show mls qos interface gigabitethernet0/7 statistics
FastEthernet1/0/7
GigabitEthernet0/7

  dscp: incoming
-------------------------------

  0 -  4 :       4213          0          0          0          0
  5 -  9 :          0          0          0          0          0
 10 - 14 :          0          0          0          0          0
 15 - 19 :          0          0          0          0          0
 20 - 24 :          0          0          0          0          0
 25 - 29 :          0          0          0          0          0
 30 - 34 :          0          0          0          0          0
 35 - 39 :          0          0          0          0          0
 40 - 44 :          0          0          0          0          0
 45 - 49 :          0          0          0          6          0
 50 - 54 :          0          0          0          0          0
 55 - 59 :          0          0          0          0          0
 60 - 64 :          0          0          0          0
  dscp: outgoing
-------------------------------

  0 -  4 :     363949          0          0          0          0
  5 -  9 :          0          0          0          0          0
 10 - 14 :          0          0          0          0          0
 15 - 19 :          0          0          0          0          0
 20 - 24 :          0          0          0          0          0
 25 - 29 :          0          0          0          0          0
 30 - 34 :          0          0          0          0          0
 35 - 39 :          0          0          0          0          0
 40 - 44 :          0          0          0          0          0
 45 - 49 :          0          0          0          0          0
 50 - 54 :          0          0          0          0          0
```

```
 55 - 59 :          0          0          0          0          0
 60 - 64 :          0          0          0          0
  cos: incoming
-------------------------------

  0 -  4 :     132067          0          0          0          0
  5 -  9 :          0          0          0
  cos: outgoing
-------------------------------

  0 -  4 :     739155          0          0          0          0
  5 -  9 :         90          0          0

Policer: Inprofile:        0 OutofProfile:        0
```

Table 2-24 show mls qos interface statistics Field Descriptions

Field		Description
DSCP	incoming	Number of received packets for each DSCP value.
	outgoing	Number of sent packets for each DSCP value.
CoS	incoming	Number of received packets for each CoS value.
	outgoing	Number of sent packets for each CoS value.
Policer	Inprofile	Number of in profile packets for each policer.
	Outofprofile	Number of out of profile packets for each policer.

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
mls qos srr-queue input bandwidth	Assigns shaped round robin (SRR) weights to an ingress queue.
mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
mls qos srr-queue input cos-map	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue input dscp-map	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue input threshold	Assigns WTD threshold percentages to an ingress queue.
mls qos srr-queue output cos-map	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
policy-map	Creates or modifies a policy map.
priority-queue	Enables the egress expedite queue on an interface.
queue-set	Maps a port to a queue-set.
srr-queue bandwidth limit	Limits the maximum output on a port.

Command	Description
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

show mls qos maps

Use the **show mls qos maps** user EXEC command to display quality of service (QoS) mapping information. During classification, QoS uses the mapping tables to represent the priority of the traffic and to derive a corresponding class of service (CoS) or Differentiated Services Code Point (DSCP) value from the received CoS, DSCP, or IP precedence value.

show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

cos-dscp	(Optional) Display class of service (CoS)-to-DSCP map.
cos-input-q	(Optional) Display the CoS input queue threshold map.
cos-output-q	(Optional) Display the CoS output queue threshold map.
dscp-cos	(Optional) Display DSCP-to-CoS map.
dscp-input-q	(Optional) Display the DSCP input queue threshold map.
dscp-mutation *dscp-mutation-name*	(Optional) Display the specified DSCP-to-DSCP-mutation map.
dscp-output-q	(Optional) Display the DSCP output queue threshold map.
ip-prec-dscp	(Optional) Display the IP-precedence-to-DSCP map.
policed-dscp	(Optional) Display the policed-DSCP map.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

The policed-DSCP, DSCP-to-CoS, and the DSCP-to-DSCP-mutation maps are displayed as a matrix. The d1 column specifies the most-significant digit in the DSCP. The d2 row specifies the least-significant digit in the DSCP. The intersection of the d1 and d2 values provides the policed-DSCP, the CoS, or the mutated-DSCP value. For example, in the DSCP-to-CoS map, a DSCP value of 43 corresponds to a CoS value of 5.

The DSCP input queue threshold and the DSCP output queue threshold maps are displayed as a matrix. The d1 column specifies the most-significant digit of the DSCP number. The d2 row specifies the least-significant digit in the DSCP number. The intersection of the d1 and the d2 values provides the queue ID and threshold ID. For example, in the DSCP input queue threshold map, a DSCP value of 43 corresponds to queue 2 and threshold 1 (02-01).

The CoS input queue threshold and the CoS output queue threshold maps show the CoS value in the top row and the corresponding queue ID and threshold ID in the second row. For example, in the CoS input queue threshold map, a CoS value of 5 corresponds to queue 2 and threshold 1 (2-1).

Examples

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

```
Switch> show mls qos maps
Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07

Cos-dscp map:
     cos:   0  1  2  3  4  5  6  7
   --------------------------------
    dscp:   0  8 16 24 32 40 48 56

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   0  8 16 24 32 40 48 56

Dscp-outputq-threshold map:
  d1 :d2    0     1     2     3     4     5     6     7     8     9
  ------------------------------------------------------------------------
   0 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
   1 :    02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01 03-01
   2 :    03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
   3 :    03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01 04-01
   5 :    04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   6 :    04-01 04-01 04-01 04-01
```

```
Dscp-inputq-threshold map:
    d1 :d2    0     1     2     3     4     5     6     7     8     9
    ------------------------------------------------------------------
     0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     2 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     3 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01 01-01
     5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
     6 :    01-01 01-01 01-01 01-01

Cos-outputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1

   Cos-inputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1

Dscp-dscp mutation map:
   Default DSCP Mutation Map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

Related Commands

Command	Description
mls qos map	Defines the CoS-to-DSCP map, DSCP-to-CoS map, DSCP-to-DSCP-mutation map, IP-precedence-to-DSCP map, and the policed-DSCP map.
mls qos srr-queue input cos-map	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue input dscp-map	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
mls qos srr-queue output cos-map	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.

show mls qos queue-set

Use the **show mls qos queue-set** user EXEC command to display quality of service (QoS) settings for the egress queues.

show mls qos queue-set [*qset-id*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

qset-id	(Optional) ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mls qos queue-set** command:

```
Switch> show mls qos queue-set
Queueset: 1
Queue    :        1       2       3       4
----------------------------------------------
buffers  :       25      25      25      25
threshold1:      100      50      100     100
threshold2:      100      50      100     100
reserved :       50      100      50      50
maximum  :       400     400     400     400
Queueset: 2
Queue    :        1       2       3       4
----------------------------------------------
buffers  :       25      25      25      25
threshold1:      100      50      100     100
threshold2:      100      50      100     100
reserved :       50      100      50      50
maximum  :       400     400     400     400
```

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to the queue-set.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation of the queue-set.

show monitor

Use the **show monitor** user EXEC command to display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch. Use the command with keywords to show a specific session, all sessions, all local sessions, or all remote sessions.

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

session	(Optional) Display information about specified SPAN sessions.
session_number	Specify the number of the SPAN or RSPAN session. The range is 1 to 66.
all	Display all SPAN sessions.
local	Display only local SPAN sessions.
range *list*	Display a range of SPAN sessions, where *list* is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges. **Note** This keyword is available only in privileged EXEC mode.
remote	Display only remote SPAN sessions.
detail	(Optional) Display detailed information about the specified sessions.
| begin	Display begins with the line that matches the *expression*.
| exclude	Display excludes lines that match the *expression*.
| include	Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **range** *list* and **detail** keywords were added.

Usage Guidelines

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

The output is the same for the **show monitor** command and the **show monitor session all** command.

Examples

This is an example of output for the **show monitor** user EXEC command:

```
Switch# show monitor
Session 1
---------
 Type       :Local Session
Source Ports:
    RX Only:      Fa4/0/24 Gi0/24
    TX Only:      None
    Both:         Fa2/0/1-2,Fa4/0/1-5 Gi0/1-2,Gi0/4-5
Source VLANs:
    RX Only:      None
    TX Only:      None
    Both:         None
Source RSPAN VLAN:None
Destination Ports:Fa2/0/18 Gi0/10
    Encapsulation:Replicate
Filter VLANs:     None
Dest RSPAN VLAN:  None

Session 2
---------
 Type       :Remote Source Session
Source Ports:
    RX Only:      None
    TX Only:      None
    Both:         None
Source VLANs:
    RX Only:      None
    TX Only:      10
    Both:         1-9
Source RSPAN VLAN:None
Destination Ports:None
Filter VLANs:     None
Dest RSPAN VLAN:  105
```

This is an example of output for the **show monitor** user EXEC command for RSPAN source session 1:

```
Switch# show monitor session 1
Session 1
---------
 Type       :Local Session
Source Ports:
    RX Only:      Fa4/0/24 Gi0/24
    TX Only:      None
    Both:         Fa2/0/1-2,Fa4/0/1-5 Gi0/1-2,Gi0/4-5
Source VLANs:
    RX Only:      None
    TX Only:      None
    Both:         None
Source RSPAN VLAN:None
Destination Ports:Fa2/0/18 Gi0/10
    Encapsulation:Replicate
Filter VLANs:     None
Dest RSPAN VLAN:  None
```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```
Switch# show monitor session all
Session 1
---------
Type               :Local Session
Source Ports       :
    Both           :Fa1/0/2 Gi0/2
Destination Ports :Fa2/0/2 Gi0/3
    Encapsulation :Replicate
          Ingress:Enabled, default VLAN = 5
    Ingress encapsulation:DOT1Q

Session 2
---------
Type               :Local Session
Source Ports       :
    Both           :Fa3/0/2 Gi0/5
Destination Ports :Fa3/0/4 Gi0/7
    Encapsulation :Replicate
          Ingress:Enabled
    Ingress encapsulation:ISL
```

Related Commands

Command	Description
monitor session	Starts or modifies a SPAN or RSPAN session.

show mvr

Use the **show mvr** privileged EXEC command without keywords to display the current 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 *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the preceding display, the maximum number of multicast groups is fixed at 256. The MVR mode is either compatible (for inter-operability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with IGMP snooping operation and dynamic MVR membership on source ports is supported).

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **interface** and **members** keywords are appended to the command.
show mvr members	Displays all ports that are members of an MVR multicast group or, if there are no members, means the group is inactive.

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

interface-id	(Optional) Display MVR type, status, and Immediate Leave setting for the interface. Valid interfaces include physical ports (including type, stack member, module, and port number.
members	(Optional) Display all MVR groups to which the specified interface belongs.
vlan *vlan-id*	(Optional) Display all MVR group members on this VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	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.

If you enter the **members** keyword, all MVR group members on the interface are displayed. If you enter a VLAN ID, all MVR group members in the VLAN are displayed.

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

Examples

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

```
Switch# show mvr interface
Port      Type            Status          Immediate Leave
----      ----            -------         ---------------
Gi1/0/1     SOURCE          ACTIVE/UP       DISABLED
Gi1/0/2     RECEIVER        ACTIVE/DOWN     DISABLED
Gi1/0/5     RECEIVER        ACTIVE/UP       ENABLED
```

In the preceding display, Status is defined as follows:

- 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 yet part of any VLAN.

This is an example of output from the **show mvr interface gigabitethernet 1/0/2** command:

```
Switch# show mvr interface gigabitethernet1/0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This is an example of output from the **show mvr interface gigabitethernet1/0/6 members** command:

```
Switch# show mvr interface gigabitethernet1/0/6 members
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 (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
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

ip-address	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group are displayed. 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 Inactive.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	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* are not displayed, but the lines that contain *Output* are displayed.

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          Gi1/0/1(d), Gi1/0/5(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 members 239.255.0.2
239.255.003.--22     ACTIVE          Gi1/0/1(d), Gi1/0/2(d), Gi1/0/3(d),
                                     Gi1/0/4(d), Gi1/0/5(s)
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
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 when the **members** keyword is appended to the command.

show pagp

Use the **show pagp** user EXEC command to display Port Aggregation Protocol (PAgP) channel-group information.

show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**} [| {**begin** | **exclude** | **include**} *expression*]]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 12.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

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

Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
  Gi1/0/1    45     42       0      0
  Gi1/0/2    45     41       0      0
  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
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/1     SC    U6/S7   H       30s      1         128        Any      16
Gi1/0/2     SC    U6/S7   H       30s      1         128        Any      16
Gi0/1       SC    U6/S7   H       30s      1         128        Any      16
Gi0/2       SC    U6/S7   H       30s      1         128        Any      16
```

This is an example of output from the **show pagp 1 neighbor** command:

```
Switch> show pagp 1 neighbor
    Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
            A - Device is in Auto mode.        P - Device learns on physical port.

    Channel group 1 neighbors
                Partner             Partner          Partner           Partner Group
    Port        Name                Device ID        Port         Age  Flags   Cap.
    Gi0/1       vegas-p2            0002.4b29.4600   Gi0/1          9s SC      10001
    Gi0/2       vegas-p2            0002.4b29.4600   Gi0/2         24s SC      10001
```

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.

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-map-name*]] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

policy-map-name	(Optional) Display the specified policy-map name.
class *class-map-name*	(Optional) Display QoS policy actions for a individual class.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **interface** keyword is not supported, and the statistics shown in the display should be ignored.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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

```
Switch> show policy-map
Policy Map videowizard_policy2
  class  videowizard_10-10-10-10
   set ip dscp 34
   police 100000000 2000000 exceed-action drop

 Policy Map mypolicy
  class  dscp5
   set ip dscp 6
```

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 port-security settings for an interface or for the switch.

show port-security [**interface** *interface-id*] [**address** | **vlan**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, stack member, module, and port number).
address	(Optional) Display all secure MAC addresses on all ports or a specified port.
vlan	(Optional) Display port security settings for all VLANs on the specified interface. This keyword is visible only on interfaces that have the switchport mode set to **trunk**.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **vlan** keyword was added (visible only on trunk ports).

Usage Guidelines

If you enter the command without keywords, the output includes the administrative and operational status of all secure ports on the switch.

If you enter an *interface-id*, the 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.

If you enter the **vlan** keyword, the **show port-security address interface** *interface-id* **vlan** command displays the configured maximum and the current number of secure MAC addresses for all VLANs on the interface. This option is visible only on interfaces that have the switchport mode set to **trunk**.

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

Examples

This is an example of the output from the **show port-security** command:

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
---------------------------------------------------------------------------
     Gi1/  0/1         1             0             0             Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

This is an example of output from the **show port-security interface gigabitethernet1/0/1** command:

```
Switch# show port-security interface gigabitethernet1/0/1
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
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    0006.0700.0800    SecureConfigured    Gi1/  0/2     1
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

This is an example of output from the **show port-security interface gigabitethernet1/0/2 address** command:

```
Switch# show port-security interface gigabitethernet1/0/2 address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi1/  0/2     1
------------------------------------------------------------------
Total Addresses: 1
```

This is an example of output from the **show port-security interface gigabitethernet1/0/2 vlan** command:

```
Switch# show port-security interface gigabitethernet1/0/2 vlan
Default maximum:not set, using 5120
VLAN  Maximum    Current
    5    default          1
   10    default         54
   11    default        101
   12    default        101
   13    default        201
   14    default        501
```

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 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

vlan-ids	(Optional) Display configuration information for a single VLAN identified by VLAN ID number or a range of VLANs separated by a hyphen. For *vlan-id*, the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show running-config vlan** command:

```
Switch# show running-config vlan 220-2000
Building configuration...

Current configuration:
!
vlan 239
!
vlan 501
!
vlan 1000
!
vlan 1002
 tb-vlan1 1
 tb-vlan2 1003
!
vlan 1003
 tb-vlan1 1
 tb-vlan2 1002
!
vlan 1004
 bridge 1
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 sdm prefer

Use the **show sdm prefer** privileged EXEC command to display information about the Switch Database Management (SDM) templates that can be used to maximize used for allocating system resources for a particular feature, or use the command without a keyword to display the template in use.

show sdm prefer [**default** | **routing** | **vlan** [**desktop**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

default	(Optional) Display the template that balances system resources among features.
routing	(Optional) Display the template that maximizes system resources for routing.
vlan	(Optional) Display the template that maximizes system resources for Layer 2 VLANs.
desktop	(Optional) For Catalyst 3750-12S aggregator switches only, display the desktop templates. For this switch, when you do not enter the **desktop** keyword, the aggregator templates appear.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **desktop** keyword was added.

Usage Guidelines

When you change the SDM template by using the **sdm prefer** global configuration command, you must reload the switch for the configuration to take effect. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

The numbers displayed for each the template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured.

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

Examples

This is an example of output from the **show sdm prefer** command, displaying the template in use:

```
Switch# show sdm prefer
"default" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:            12K
  number of igmp groups + multicast routes:   1K
  number of unicast routes:                   0
  number of qos aces:                         512
  number of security aces:                    1K
Switch# show sdm prefer
 The current template is "desktop default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:            6K
  number of igmp groups + multicast routes:   1K
  number of unicast routes:                   8K
    number of directly connected hosts:       6K
    number of indirect routes:                2K
  number of policy based routing aces:        0
  number of qos aces:                         512
  number of security aces:                    1K
```

This is an example of output from the **show sdm prefer routing** command entered on an aggregator switch:

```
Switch# show sdm prefer routing
"aggregate routing" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:            6K
  number of igmp groups + multicast routes:   1K
  number of unicast routes:                   20K
    number of directly connected hosts:       6K
    number of indirect routes:                14K
  number of policy based routing aces:        512
  number of qos aces:                         512
  number of security aces:                    1K
```

This is an example of output from the **show sdm prefer routing** command entered on a desktop switch:

```
Switch# show sdm prefer routing
"desktop routing" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:            3K
  number of igmp groups + multicast routes:   1K
  number of unicast routes:                   11K
    number of directly connected hosts:       3K
    number of indirect routes:                8K
  number of policy based routing aces:        512
  number of qos aces:                         512
  number of security aces:                    1K
```

This is an example of output from the **show sdm prefer** command when you have configured a new template but have not reloaded the switch:

```
Switch# show sdm prefer
 The current template is "desktop routing" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:            3K
  number of igmp groups + multicast routes:   1K
  number of unicast routes:                   11K
    number of directly connected hosts:       3K
    number of indirect routes:                8K
  number of qos aces:                         512
  number of security aces:                    1K

 On next reload, template will be "aggregate routing" template.
```

Related Commands

Command	Description
sdm prefer	Sets the SDM template to maximize resources for routing or VLANs or to the default template, or to select the desktop or aggregator templates.

show setup express

Use the **show setup express** privileged EXEC command to display if Express Setup mode is active on the switch.

show setup express [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

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.
setup express	Enables Express Setup mode.

show spanning-tree

Use the **show spanning-tree** user EXEC command to display spanning-tree state information.

show spanning-tree [*bridge-group* | **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 *bridge-group* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**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-group*} **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **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

bridge-group	(Optional) Specify the bridge group number. The range is 1 to 255.
active [**detail**]	(Optional) Display spanning-tree information only on active interfaces (available only in privileged EXEC mode).
backbonefast	(Optional) Display spanning-tree BackboneFast status.
blockedports	(Optional) Display blocked port information (available only 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 available only in privileged EXEC mode).
detail [**active**]	(Optional) Display a detailed summary of interface information (**active** keyword available only in privileged EXEC mode).
inconsistentports	(Optional) Display inconsistent port information (available only in privileged EXEC mode).
interface *interface-id* [**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** available only 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 VLAN range is 1 to 4094. The port-channel range is 1 to 12.

mst [**configuration** | [*instance-id* [**detail** | **interface** *interface-id* [**detail**]]	(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode). You can specify a single instance ID, a range of IDs separated by a hyphen, or a series of IDs separated by a comma. The range is 1 to 15. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 64.
pathcost method	(Optional) Display the default path cost method (available only 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 available only 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 *vlan-id* [**active** [**detail**] | **backbonefast** | **blockedports** | **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display spanning-tree information for the specified VLAN (some keywords available only in privileged EXEC mode). 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.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC; indicated keywords available only in privileged EXEC mode.

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **mst** keyword and options were added.

Usage Guidelines

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs.

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

Examples

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0001.42e2.cdd0
             Cost        3038
             Port        24 (GigabitEthernet2/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49153  (priority 49152 sys-id-ext 1)
             Address     0003.fd63.9580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi2/0/1          Root FWD 3019      128.24   P2p
<output truncated>
```

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 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 24 (GigabitEthernet2/0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h 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
  Uplinkfast enabled

 Port 1 (GigabitEthernet2/0/1) of VLAN0001 is forwarding
   Port path cost 3019, Port priority 128, Port Identifier 128.24.
   Designated root has priority 32768, address 0001.42e2.cdd0
   Designated bridge has priority 32768, address 00d0.bbf5.c680
   Designated port id is 128.25, designated path cost 19
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 0, received 72364
<output truncated>
```

This is an example of output from the **show spanning-tree interface gigabitethernet2/0/1** command:

```
Switch# show spanning-tree interface gigabitethernet2/0/1
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 3019      128.24   P2p

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 enabled
BackboneFast         is enabled
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                  1        0         0        11         12
VLAN0002                  3        0         0        1          4
VLAN0004                  3        0         0        1          4
VLAN0006                  3        0         0        1          4
VLAN0031                  3        0         0        1          4
VLAN0032                  3        0         0        1          4
<output truncated>
---------------------- -------- --------- -------- ---------- ----------
37 vlans                  109      0         0        47         156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----------------------
Number of transitions via uplinkFast (all VLANs)            : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs)           : 0
Number of inferior BPDUs received (all VLANs)               : 0
Number of RLQ request PDUs received (all VLANs)             : 0
Number of RLQ response PDUs received (all VLANs)            : 0
Number of RLQ request PDUs sent (all VLANs)                 : 0
Number of RLQ response PDUs sent (all VLANs)                : 0
```

This is an example of output from the **show spanning-tree mst configuration** command:

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ------------------
0         1-9,21-4094
1         10-20
-----------------------------
```

This is an example of output from the **show spanning-tree mst interface gigabitethernet2/0/1** command:

```
Switch# show spanning-tree mst interface gigabitethernet2/0/1
GigabitEthernet2/0/1 of MST00 is root forwarding
Edge port: no             (default)        port guard : none        (default)
Link type: point-to-point (auto)           bpdu filter: disable     (default)
Boundary : boundary       (STP)            bpdu guard : disable     (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
0        root FWD   200000    128  1,12,14-4094
```

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
###### MST00        vlans mapped: 1-9,21-4094
Bridge      address 0002.4b29.7a00  priority  32768 (32768 sysid 0)
Root        address 0001.4297.e000  priority  32768 (32768 sysid 0)
            port    Gi1/0/1         path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface              role state cost      prio type
---------------------  ---- ----- --------- ---- --------------------------------
GigabitEthernet2/0/1   root FWD   200000    128  P2P bound(STP)
GigabitEthernet2/0/2   desg FWD   200000    128  P2P bound(STP)
Port-channel1          desg FWD   200000    128  P2P bound(STP)
```

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 bpdufilter	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree extend system-id	Enables the extended system ID feature.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree link-type	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
spanning-tree loopguard default	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
spanning-tree mst configuration	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.

Command	Description
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in an MST region before the BPDU is discarded and the information held for a port is aged.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.
spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
spanning-tree vlan	Configures spanning tree on a per-VLAN basis.

show storm-control

Use the **show storm-control** user EXEC command to display broadcast, multicast, or unicast storm control settings on the switch or on the specified interface or to display storm-control history.

show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Interface ID for the physical port (including type, stack member, module, and port number).
broadcast	(Optional) Display broadcast storm threshold setting.
multicast	(Optional) Display multicast storm threshold setting.
unicast	(Optional) Display unicast storm threshold setting.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

When you enter an *interface-id*, the storm control thresholds are displayed for the specified interface.

If you do not enter an *interface-id*, settings are displayed for one traffic type for all ports on the switch.

If you do not enter a traffic type, settings are displayed for broadcast storm control.

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

Examples

This is an example of a partial output from the **show storm-control** command when no keywords are entered. Because no traffic type keyword was entered, the broadcast storm control settings are displayed.

```
Switch> show storm-control

Interface  Filter State   Level    Current
---------  -------------  -------  -------
Gi1/0/1      inactive       100.00%  N/A
Gi1/0/2      inactive       100.00%  N/A
Gi1/0/3      inactive       100.00%  N/A
Gi1/0/4      inactive       100.00%  N/A
Gi1/0/5      inactive       100.00%  N/A
Gi1/0/6      inactive       100.00%  N/A
Gi1/0/7      inactive       100.00%  N/A
Gi1/0/8      inactive       100.00%  N/A
```

```
Gi1/0/9       inactive       100.00%  N/A
Gi1/0/10      inactive       100.00%  N/A
Gi1/0/11      inactive       100.00%  N/A
Gi1/0/12      inactive       100.00%  N/A
Gi1/0/13      inactive       100.00%  N/A
Gi1/0/14      inactive       100.00%  N/A

<output truncated>
```

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic type keyword was entered, the broadcast storm control settings are displayed.

```
Switch> show storm-control gigabitethernet 2/0/1

Interface  Filter State   Level    Current
---------  -------------  -------  -------
Gi2/0/1      inactive       100.00%  N/A
```

This is an example of output from the **show storm-control** command for a specified interface and traffic type, where no storm control threshold has been set for that traffic type on the specified interface.

```
Switch> show storm-control gigabitethernet1/0/5 multicast

Interface  Filter State   Level    Current
---------  -------------  -------  -------
Gi1/0/5      inactive       100.00%  N/A
```

Table 2-25 describes the fields in the **show storm-control** display.

Table 2-25 show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: • Blocking—Storm control is enabled, and a storm has occurred. • Forwarding—Storm control is enabled, and no storms have occurred. • Inactive—Storm control is disabled.
Level	Displays the threshold level set on the interface for broadcast traffic or the specified traffic type (broadcast, multicast, or unicast).
Current	Displays the bandwidth utilization of broadcast traffic or the specified traffic type (broadcast, multicast, or unicast) as a percentage of total available bandwidth. This field is only valid when storm control is enabled.

Related Commands

Command	Description
storm-control	Sets the broadcast, multicast, or unicast storm control levels for the switch.

show switch

Use the **show switch** user EXEC command to display information related to the stack member or the switch stack.

show switch [*stack-member-number* | **detail** | **neighbors** | **stack-ports**] [| {**begin** | **exclude** | **include**} *expression*

Syntax Description

stack-member-number	(Optional) Display information for the specified stack member. The range is 1 to 9.
detail	(Optional) Display detailed information about the stack ring.
neighbors	(Optional) Display the neighbors for the entire switch stack.
stack-ports	(Optional) Display port information for the entire switch stack.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The output for this command was expanded to include Switch Database Management (SDM) mismatch.

Usage Guidelines

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

These are the states displayed from this command:

- Waiting—The stage when a switch is booting up and waiting for communication from other switches in the stack. The switch has not yet determined whether it is a stack master or not.

  Stack members not participating in a stack master election remain in the waiting state until the stack master is elected and ready.
- Initializing—The stage when a switch has determined whether it is the stack master or not. If the switch is not the stack master, it is receiving its system- and interface-level configuration from the stack master and loading it.
- Ready—The stage when the stack member has completed loading the system- and interface-level configuration and is ready to forward traffic.
- Master Re-Init—The stage immediately after a stack master re-election and a different stack member is elected stack master. The new stack master is re-initializing its configuration. This state applies only to the new stack master.

- Ver Mismatch—The stage of a switch in version mismatch (VM) mode. VM mode is when a switch joining the switch stack has a different stack protocol minor version number from the stack master.
- SDM Mismatch—The stage of a switch in Switch Database Management (SDM) mismatch mode. SDM mismatch is when a stack member does not support the SDM template running on the stack master.

A typical state transition for a stack member (including a stack master) booting up is Waiting -> Initializing -> Ready.

A typical state transition for a stack member becoming a stack master after a stack master election is Ready -> Master Re-Init -> Ready.

A typical state transition for a stack member in version mismatch (VM) mode is Waiting -> Ver Mismatch.

The word *slave* in the output refers to a stack member other than the stack master.

Examples

This example shows how to display summary information about stack member 6:

```
Switch(config)# show switch 6
                                                     Current
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------------
 6       Slave     0003.e31a.1e00     1         Ready
```

This example shows how to display summary information about a switch stack:

```
Switch(config)# show switch
                                                     Current
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------------
 6       Slave     0003.e31a.1e00     1         Ready
*8       Master    0003.e31a.1200     1         Ready
```

This example shows detailed information about a switch stack:

```
Switch(config)# show switch detail
                                                     Current
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------------
 6       Slave     0003.e31a.1e00     1         Ready
*8       Master    0003.e31a.1200     1         Ready

         Stack Port Status             Neighbors
Switch#  Port A     Port B           Port A   Port B
-----------------------------------------------------------
  6       Down        Ok              None       8
  8        Ok        Down               6      None
```

This example shows how to display neighbor information for a switch stack:

```
Switch(config)# show switch neighbors
  Switch #    Port A       Port B
  --------    ------       ------
      6        None           8
      8         6            None
```

This example shows how to display stack-port information for a switch stack:

```
Switch(config)# show switch stack-ports
  Switch #    Port A       Port B
  --------    ------       ------
    6           Down         Ok
    8            Ok          Down
```

Related Commands

Command	Description
reload	Saves the configuration change and restarts the stack member.
remote command	Monitors all or specified stack members.
session	Accesses a specific stack member.
switch priority	Changes the stack member priority value.
switch renumber	Changes the stack member number.

show system mtu

Use the **show system mtu** privileged EXEC command to display the global maximum transmission unit (MTU) or maximum packet size set for the switch.

show system mtu [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

If you have used the **system mtu** or **system mtu jumbo** global configuration command to change the MTU setting, the new setting does not take effect until you reset the switch.

The system MTU refers to 10/100 ports; the system jumbo MTU refers to Gigabit ports.

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

Examples

This is an example of output from the **show system mtu** command:

```
Switch# show system mtu

System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
```

Related Commands

Command	Description
system mtu	Sets the MTU size for the Fast Ethernet or Gigabit Ethernet ports.

show udld

Use the **show udld** user EXEC command to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

show udld [*interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

If you do not enter an *interface-id*, administrative and operational UDLD status for all interfaces are displayed.

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

Examples

This is an example of output from the **show udld gigabitethernet6/0/11** command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-26 describes the fields in this display.

```
Switch> show udld gigabitethernet6/0/11
Interface gi6/0/11
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
    Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: 0050e2826000
    Port ID: Gi6/0/12
    Neighbor echo 1 device: SAD03160954
    Neighbor echo 1 port: Gi6/0/11
    Message interval: 5
    CDP Device name: 066527791
```

Table 2-26 show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state is displayed if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state is displayed if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
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 current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries are displayed.
Device name	The neighbor MAC address.
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The MAC address of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	CDP name of the device.

Related Commands

Command	Description
udld (global configuration)	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld (interface configuration)	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again.

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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

```
Switch> show version
Cisco Internetwork Operating System Software
IOS (tm) C3750 Software (C3750-I5-M), Version 12.1(0.0.709)EA1, CISCO DEVELOPMENT TEST
VERSION
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Fri 02-May-03 21:09 by antonino
Image text-base: 0x00003000, data-base: 0x008E36A4

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.1(0.0.130)EA1, CISCO DEVELOPMENT
TEST VERSION

Switch uptime is 2 days, 11 hours, 16 minutes
System returned to ROM by power-on
System image file is "flash:i5.709"

cisco WS-C3750-48TS (PowerPC405) processor with 120822K/10240K bytes of memory.
Last reset from power-on
Bridging software.
Target IOS Version 12.1(14)EA1
1 Virtual Ethernet/IEEE 802.3  interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
32 Gigabit Ethernet/IEEE 802.3 interface(s)
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:09:43:A7:F2:00
```

```
Motherboard assembly number     : 73-7056-05
Motherboard serial number       : CSJ0638004U
Motherboard revision number     : 05
Model number                    : 73-7056-05


Switch   Ports  Model              SW Version             SW Image
------   -----  -----              ----------             ----------
     1   28     WS-C3750G-24TS     12.1(0.0.709)EA1       C3750-I5-M
*    8   52     WS-C3750-48TS      12.1(0.0.709)EA1       C3750-I5-M


Switch 01
---------

Switch Uptime                   : 2 days, 11 hours, 17 minutes
Base ethernet MAC Address       : 00:0B:46:2E:35:80
Motherboard assembly number     : 73-7058-04
Power supply part number        : 341-0045-01
Motherboard serial number       : CSJ0640010L
Model number                    : WS-C3750-24TS-SMI
System serial number            : CSJ0642U00A

Configuration register is 0xF

<output truncated>
Switch> show version
Cisco Internetwork Operating System Software
IOS (tm) C2970 Software (C2970-I6K2L2-M), Version 12.1(0.0.711)EA1, CISCO DEVELOPMENT TEST
VERSION
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 12-May-03 15:58 by antonino
Image text-base: 0x00003000, data-base: 0x007743AC

ROM: Bootstrap program is C2970 boot loader
BOOTLDR: C2970 Boot Loader (C2970-HBOOT-M) Version 12.1(0.0.26)EA1, CISCO DEVELOPMENT TEST
VERSION

Switch uptime is 50 minutes
System returned to ROM by power-on
System image file is "flash:c2970-i6k2l2-mz"

cisco WS-C2970G-24T-E (PowerPC405) processor with 120822K/10240K bytes of memo
.
Last reset from power-on
Target IOS Version 12.1(14)EA1
1 Virtual Ethernet/IEEE 802.3  interface(s)
24 Gigabit Ethernet/IEEE 802.3 interface(s)
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0B:46:2E:58:80

Switch   Ports  Model              SW Version             SW Image
------   -----  -----              ----------             ----------
*    1   24     WS-C2970G-24T-E    12.1(0.0.711)EA1       C2970-I6K2L2-M

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* | **internal usage** | **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 *vlan-id*	(Optional) Display information about a single VLAN identified by VLAN ID number. For *vlan-id*, the range is 1 to 4094.
internal usage	(Optional) Display list of VLANs being used internally by the switch. These VLANs are always from the extended range (VLAN IDs 1006 to 4094), and you cannot create VLANs with these IDS by using the **vlan** global configuration command until you remove them from internal use.
name *vlan-name*	(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.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **ifindex**, **internal usage**, and **private-vlan** keywords are not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show vlan** command. Table 2-27 describes each field in the display.

```
Switch> show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa1/0/1, Fa1/0/2, Fa1/0/3
                                                 Fa1/0/4, Fa1/0/5, Fa1/0/6
                                                 Fa1/0/7, Fa1/0/8, Fa1/0/9
                                                 Fa1/0/10, Fa1/0/11, Fa1/0/12
                                                 Fa1/0/13, Fa1/0/14, Fa1/0/15
                                                 Fa1/0/16, Fa1/0/17, Fa1/0/18
                                                 Fa1/0/19, Fa1/0/20, Fa1/0/21
                                                 Fa1/0/22, Fa1/0/23, Fa1/0/24
                                                 Fa1/0/25, Fa1/0/26, Fa1/0/27
                                                 Fa1/0/28, Fa1/0/29, Fa1/0/30
                                                 Fa1/0/31, Fa1/0/32, Fa1/0/33
                                                 Fa1/0/34, Fa1/0/35, Fa1/0/36
                                                 Fa1/0/46, Gi1/0/1, Gi1/0/2
                                                 Gi1/0/3, Gi1/0/4, Gi2/0/1
                                                 Gi2/0/2, Gi2/0/3, Gi2/0/4
                                                 Gi2/0/5, Gi2/0/6, Gi2/0/7

<output truncated>

2    VLAN0002                          active
3    VLAN0003                          active

<output truncated>

1000 VLAN1000                          active
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
3    enet  100003     1500  -      -      -        -    -        0      0

<output truncated>

1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                 Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                 Gi0/9, Gi0/10, Gi0/11, Gi0/12
                                                 Gi0/13, Gi0/14, Gi0/15, Gi0/16
                                                 Gi0/17, Gi0/18, Gi0/19, Gi0/20
                                                 Gi0/21, Gi0/22, Gi0/23, Gi0/24
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  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Table 2-27 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.
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.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.
Primary/Secondary/ Type/Ports	Not applicable to this release.

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

```
Switch> show vlan summary
Number of existing VLANs           : 45
 Number of existing VTP VLANs      : 45
 Number of existing extended VLANs : 0
```

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

```
Switch# show vlan id 2

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Fa1/0/47, Fa1/0/48, Gi2/0/13
```

```
                                                Gi3/0/1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                Gi0/9, Gi0/10, Gi0/11, Gi0/12
                                                Gi0/13, Gi0/14, Gi0/15, Gi0/16
                                                Gi0/17, Gi0/18, Gi0/19, Gi0/20
                                                Gi0/21, Gi0/22, Gi0/23, Gi0/24

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled
```

This is an example of output from the **show vlan internal usage** command. It shows that VLANs 1025 and 1026 are being used as internal VLANs for Fast Ethernet routed ports 23 and 24 on stack member 1. If you want to use one of these VLAN IDs, you must first shut down the routed port, which releases the internal VLAN, and then create the extended-range VLAN. When you start up the routed port, another internal VLAN number is assigned to it.

```
Switch> show vlan internal usage

VLAN Usage
---- -------------
1025 FastEthernet1/0/23
1026 FastEthernet1/0/24
```

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.
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 vlan access-map

Use the **show vlan access-map** privileged EXEC command to display information about a particular VLAN access map or all VLAN access maps.

show vlan access-map [*mapname*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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

```
Switch# show vlan access-map
Vlan access-map "SecWiz"  10
  Match clauses:
    ip  address: SecWiz_Fa1_Gi0_3_in_ip
  Action:
    forward
```

Related Commands

Command	Description
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

show vlan filter

Use the **show vlan filter** privileged EXEC command to display information about all VLAN filters or about a particular VLAN or VLAN access map.

show vlan filter [**access-map** *name* | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

access-map *name*	(Optional) Display filtering information for the specified VLAN access map.
vlan *vlan-id*	(Optional) Display filtering information for the specified VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show vlan filter** command:

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

Related Commands

Command	Description
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

Examples

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 2-28 describes each field in the display.

```
Switch> show vmps statistics
VMPS Client Statistics
----------------------
VQP  Queries:               0
VQP  Responses:             0
VMPS Changes:               0
VQP  Shutdowns:             0
VQP  Denied:                0
VQP  Wrong Domain:          0
VQP  Wrong Version:         0
VQP  Insufficient Resource: 0
```

Table 2-28 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 has been assigned to a VLAN). The client keeps the denied address in the address table as a blocked address to prevent more 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 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 (privileged EXEC)	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** | **password** | **status**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **password** keyword was added.

Usage Guidelines

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

Examples

This is an example of output from the **show vtp counters** command. Table 2-29 describes each field in the display.

```
Switch> show vtp counters

VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
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
---------------- ---------------- ---------------- --------------------------
Fa1/0/47            0                0                0
Fa1/0/48            0                0                0
Gi2/0/13              0                0                0
Gi3/0/1               0                0                0
```

Table 2-29 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	Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments. Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations. These errors means that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Table 2-29 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 2-30 describes each field in the display.

```
Switch> show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 45
VTP Operating Mode              : Transparent
VTP Domain Name                 : shared_testbed1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Enabled
MD5 digest                      : 0x3A 0x29 0x86 0x39 0xB4 0x5D 0x58 0xD7
```

Table 2-30 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 2-30 show vtp status Field Descriptions (continued)

Field	Description
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from nonvolatile RAM (NVRAM) after reboot. By default, every switch is a VTP server. **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. 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. 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.
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
MD5 Digest	A 16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

Related Commands

Command	Description
clear vtp counters	Clears the VTP and pruning counters.
vtp (global configuration)	Configures the VTP filename, interface name, domain name, and mode.
vtp (VLAN configuration)	Configures the VTP domain name, password, pruning, and mode.

shutdown

Use the **shutdown** interface configuration command on the switch stack or on a standalone switch to disable an interface. Use the **no** form of this command to restart a disabled interface.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

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

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

The **shutdown** command disables all functions on the specified interface.

This command also marks the interface as unavailable. To see if an interface is disabled, use the **show interfaces** privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.

Examples

These examples show how to disable and re-enable an interface:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# shutdown

Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no shutdown
```

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

Related Commands

Command	Description
show interfaces	Displays the statistical information specific to all interfaces or to a specific interface.

shutdown vlan

Use the **shutdown vlan** global configuration command on the switch stack or on a standalone switch to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be locally shut down. The range is 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
12.1(11)AX	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

This example shows how to shutdown traffic on VLAN 2:

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

You can verify your setting by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
shutdown (config-vlan mode)	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the **vlan** *vlan-id* global configuration command).
vlan database	Enters VLAN configuration mode.

snmp-server enable traps

Use the **snmp-server enable traps** global configuration command on the switch stack or on a standalone switch to enable the switch to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS). Use the **no** form of this command to return to the default setting.

snmp-server enable traps [**bgp** | **bridge | cluster** | **config** | **copy-config** | **entity** | **envmon** [**fan | shutdown | supply | temperature**] | **flash** [**insertion | removal**] | **fru-ctrl** | **hsrp** | **mac-notification** | **port-security** [**trap-rate** *value*] | **rtr** | **snmp** [**authentication | coldstart | linkdown | linkup | warmstart**] | **stpx** | **syslog**| **vlancreate**| **vlandelete** | **vlan-membership** | **vtp**]

no snmp-server enable traps [**bgp** | **bridge | cluster** | **config** | **copy-config** | **entity** | **envmon** [**fan | shutdown | supply | temperature**] | **flash** [**insertion | removal**] | **fru-ctrl** | **hsrp** | **mac-notification** | **port-security** [**trap-rate**] | **rtr** | **snmp** [**authentication | coldstart | linkdown | linkup | warmstart**] | **stpx** | **syslog**| **vlancreate**| **vlandelete** | **vlan-membership** | **vtp**]

Syntax Description

bgp	(Optional) Enable Border Gateway Protocol (BGP) state change traps. **Note** This keyword is available only when the enhanced multilayer image is installed on the stack master.
bridge	(Optional) Generate STP bridge MIB 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) Generate environmental monitor traps.
fan	(Optional) Generate environmental fan trap.
shutdown	(Optional) Generate environmental monitor shutdown traps.
supply	(Optional) Generate environmental monitor power supply traps.
temperature	(Optional) Generate environmental monitor temperature traps.
flash	(Optional) Enable SNMP FLASH notifications.
insertion	(Optional) Generate a trap when a switch (flash) is inserted into a stack, either physically or because of a power cycle or reload.
removal	(Optional) Generate a trap when a switch (flash) is removed from a stack, either physically or because of a power cycle or reload.
fru-ctrl	(Optional) Generate entity FRU control traps. In the Catalyst 3750 switch stack, this trap refers to the insertion or removal of a switch in the stack.
hsrp	(Optional) Enable Hot Standby Router Protocol (HSRP) traps.
mac-notification	(Optional) Enable MAC address notification traps.
port-security	(Optional) Enable SNMP port security traps.
trap-rate *value*	(Optional) Set the maximum number of port-security traps sent per second. The range is from 0 to 1000; the default is 0 (no limit imposed; a trap is sent at every occurrence).

rtr	(Optional) Enable SNMP Response Time Reporter traps.
snmp	(Optional) Enable SNMP traps.
authentication	(Optional) Enable authentication trap.
coldstart	(Optional) Enable cold start trap.
linkdown	(Optional) Enable linkdown trap.
linkup	(Optional) Enable linkup trap.
warmstart	(Optional) Enable warmstart trap.
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 **snmp-server enable informs** command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** command combined with the **snmp-server host** *host-addr* **informs** command.
Though visible in the command-line help strings, the **fru-ctrl,** flash **insertion** and flash **deletion** keywords are not supported.

Defaults

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **bgp, copy-config, envmon, flash, port-security, stpx, syslog**, **vlancreate**, and **vlandelete** 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 VTP traps to the NMS:

```
Switch(config)# snmp-server enable traps vtp
```

You can verify your setting by entering the **show vtp status** 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 on the switch stack or on a standalone switch 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* [[**bgp**] [**bridge**] [**cluster**] [**config**] [**copy-config**] [**entity**] [**envmon**] [**flash**] [**fru-ctrl**] [**hsrp**] [**mac-notification**] [**port-security**] [**rtr**] [**snmp**] [**stpx**] [**syslog**] [**tty**] [**udp-port**] [**vlancreate**] [**vlandelete**] [**vlan-membership**] [**vtp**]] }

no snmp-server host *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string*

Syntax Description

host-addr	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 the Simple Network Management Protocol (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: • **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. • **noauth** (Default). The noAuthNoPriv security level. This is the default if the [**auth** | **noauth** | **priv**] keyword choice is not specified. • **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called *privacy*). **Note** The **priv** keyword is available only when the crypto (encrypted) software image is installed.
community-string	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.
bgp	(Optional) Send Border Gateway Protocol (BGP) state change traps. **Note** This keyword is available only when the enhanced multilayer image is installed on the stack master.
bridge	(Optional) Send SNMP Spanning Tree Protocol (STP) bridge MIB 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) Generate environmental monitor traps.

flash	(Optional) Enable SNMP FLASH notifications.
fru-ctrl	(Optional) Generate entity FRU control traps. In the Catalyst 3750 switch stack, this trap refers to the insertion or removal of a switch in the stack.
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) Enable SNMP STP extended MIB traps.
syslog	(Optional) Enable SNMP syslog traps.
tty	(Optional) Send Transmission Control Protocol (TCP) connection traps.
udp-port	(Optional) Configure the User Datagram Protocol (UDP) port number of the host to receive the traps.
vlancreate	(Optional) Enable SNMP VLAN-created traps.
vlandelete	(Optional) Enable SNMP VLAN-deleted traps.
vlan-membership	(Optional) Send SNMP VLAN membership traps.
vtp	(Optional) Send VLAN Trunking Protocol (VTP) traps.

Note Though visible in the command-line help strings, the **fru-ctrl** keyword is not supported.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is version 1.

If version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

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
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **bgp, copy-config, flash, port-security, 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* by using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

You can verify your settings by entering 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 enable traps	Enables SNMP notification for various trap types or inform requests.

snmp trap mac-notification

Use the **snmp trap mac-notification** interface configuration command on the switch stack or on a standalone switch to enable the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific Layer 2 interface. Use the **no** form of this command to return to the default setting.

snmp trap mac-notification {**added** | **removed**}

no snmp trap mac-notification {**added** | **removed**}

Syntax Description

added	Enable the MAC notification trap whenever a MAC address is added on this interface.
removed	Enable the MAC notification trap whenever a MAC address is removed from this interface.

Defaults

By default, the traps for both address addition and address removal are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	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 enable the **snmp-server enable traps mac-notification** and the **mac address-table notification** global configuration commands.

Examples

This example shows how to enable the MAC notification trap when a MAC address is added to Gigabit Ethernet interface1/ 0/4 on stack member 1:

```
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# snmp trap mac-notification added
```

You can verify your settings by entering the **show mac address-table notification interface** 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 address notification feature.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended.
snmp-server enable traps	Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended.

spanning-tree backbonefast

Use the **spanning-tree backbonefast** global configuration command on the switch stack or on a standalone switch to enable the BackboneFast feature. Use the **no** form of the 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(11)AX	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 operating in the rapid-PVST+ or multiple spanning-tree (MST) mode.

BackboneFast starts when a root port or blocked port on a switch receives inferior BPDUs from its designated switch. An inferior BPDU identifies a switch that declares itself as both the root bridge and the designated switch. 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 switch has lost its connection to the root switch. If there are alternate paths to the root switch, BackboneFast causes the maximum aging time on the ports on which it received the inferior BPDU to expire and allows a blocked port to move immediately to the listening state. BackboneFast then transitions the interface to the forwarding state. For more information, refer to the software configuration guide for this release.

Enable BackboneFast on all supported switches to allow the detection of indirect link failures and to start the spanning-tree reconfiguration sooner.

Examples

This example shows how to enable BackboneFast on the switch:

```
Switch(config)# spanning-tree backbonefast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of the spanning-tree port states.

spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** interface configuration command on the switch stack or on a standalone switch to prevent a port from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

Syntax Description

disable	Disable BPDU filtering on the specified interface.
enable	Enable BPDU filtering on the specified interface.

Defaults

BPDU filtering is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	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 the multiple spanning-tree (MST) mode.

Caution Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled ports by using the **spanning-tree portfast bpdufilter default** global configuration command.

You can use the **spanning-tree bpdufilter** interface configuration command to override the setting of the **spanning-tree portfast bpdufilter default** global configuration command.

Examples

This example shows how to enable the BPDU filtering feature on a port on stack member 2:

```
Switch(config)# interface fastethernet2/0/1
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands**.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command on the switch stack or on a standalone switch 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(11)AX	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.

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 on stack member 2:

```
Switch(config)# interface fastethernet2/0/1
Switch(config)# interface gigabitethernet0/1
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 on the switch stack or on a standalone switch 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 *vlan-id*	(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.
cost	Path cost. The range is 1 to 200000000, with higher values meaning higher costs.

Defaults

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

- 1000 Mbps—4
- 100 Mbps—19
- 10 Mbps—100

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The value for the *vlan-id* variable was changed.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

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 the path cost to 250 on an interface on stack member 2:

```
Switch(config)# interface fastethernet2/0/4
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost to 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 *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command on the switch stack or on a standalone switch 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(11)AX	This command was first introduced.

Usage Guidelines

The Catalyst 3750Catalyst 2970 switch supports the 802.1T spanning-tree extensions. 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 rapid PVST+ or an instance identifier for the multiple spanning tree [MST]).

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. Because the Catalyst 3750 switch stack appears as a single switch to the rest of the network, all switches in the stack use the same bridge ID for a given spanning tree. If the stack master fails, the stack members recalculate their bridge IDs of all running spanning trees based on the new MAC address of the stack master.

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.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of spanning-tree port states.
spanning-tree mst root	Configures the 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 on the switch stack or on a standalone switch 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(11)AX	This command was first introduced.

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.

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 the 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 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 on stack member 2:

```
Switch(config)# interface fastethernet2/0/3
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified interface on stack member 2:

```
Switch(config)# interface fastethernet2/0/3
Switch(config)# interface gigabitethernet0/3
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 on the switch stack or on a standalone switch to override the default link-type setting, which is determined by the duplex mode of the port, and to enable rapid spanning-tree 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(14)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 rapid transitions to the forwarding state:

```
Switch(config-if)# spanning-tree link-type shared
```

You can verify your setting by entering the **show spanning-tree mst interface** *interface-id* or the show **spanning-tree interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
clear spanning-tree detected-protocols	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.
show spanning-tree interface *interface-id*	Displays spanning-tree state information for the specified interface.
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 on the switch stack or on a standalone switch 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(11)AX	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.

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 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 on the switch stack or on a standalone switch 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).
pvst	Enable PVST+ (based on IEEE 802.1D).
rapid-pvst	Enable rapid PVST+ (based on IEEE 802.1W).

Defaults

The default mode is PVST+.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **mst** and **rapid-pvst** keywords were 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. All stack members run the same version of spanning-tree.

When you enable the MST mode, RSTP is automatically enabled.

Caution Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

Examples

This example shows to enable MST and RSTP 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 on the switch stack or on a standalone switch 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

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(14)EA1	This command was first introduced.

Usage Guidelines

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 stack 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 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 VLANs 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 on the switch stack or on a standalone switch 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**

Syntax Description

instance-id	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.
cost	Path cost is 1 to 200000000, with higher values meaning higher costs.

Defaults

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

- 1000 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When you configure the cost, higher values represent higher costs.

Examples

This example shows how to set a path cost of 250 on an interface associated with instances 2 and 4:

```
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	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 on the switch stack or on a standalone switch 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

Syntax Description

seconds	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(14)EA1	This command was first introduced.

Usage Guidelines

Changing the **spanning-tree mst forward-time** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:

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

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

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 on the switch stack or on a standalone switch 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

Syntax Description

seconds	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(14)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 multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst hello-time 3
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays 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 on the switch stack or on a standalone switch 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

Syntax Description

seconds	Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds.

Defaults

The default is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)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 max-age** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:

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

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays 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 on the switch stack or on a standalone switch 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

Syntax Description

hop-count	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(14)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 multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command on the switch stack or on a standalone switch 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**

Syntax Description

instance-id	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.
priority	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(14)EA1	This command was first introduced.

Usage Guidelines

You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

If your switch is a member of a switch stack, you must use the **spanning-tree mst** [*instance-id*] **cost** *cost* interface configuration command instead of the **spanning-tree mst** [*instance vlan-id*] **port-priority** *priority* interface configuration command to select an interface to put in the forwarding state. Assign lower cost values to interfaces that you want selected first and higher cost values to interfaces that you want selected last.

Examples

This example shows how to increase the likelihood that the interface associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# spanning-tree mst 20,22 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
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command on the switch stack or on a standalone switch 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**

Syntax Description

instance-id	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.
priority	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(14)EA1	This command was first introduced.

Examples

This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instances (MST) 20 to 21:

```
Switch(config)# spanning-tree mst 20-21 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 *instance-id*	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 on the switch stack or on a standalone switch 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 settings.

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

Syntax Description

instance-id	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 *net-diameter*	(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 *seconds*	(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(14)EA1	This command was first introduced.

Usage Guidelines

Use the **spanning-tree mst** *instance-id* **root** command 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 *instance-id*	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 on the switch stack or on a standalone switch 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 *vlan-id*	(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.
priority	Number from 0 to 240, in increments of 16. Valid 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(14)EA1	The value for the *vlan-id* variable was changed. The priority range values 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.

If your switch is a member of a switch stack, you must use the **spanning-tree** [**vlan** *vlan-id*] **cost** *cost* interface configuration command instead of the **spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority* interface configuration command to select an interface to put in the forwarding state. Assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last.

Examples

This example shows how to increase the likelihood that FastGigabit Ethernet interface 0/2 on stack member 2 will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface fastethernet2/0/2
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

This example shows how to set the port-priority value on VLANs 20 to 25:

```
Switch(config-if)# spanning-tree vlan 20-25 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 *interface-id*	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 on the switch stack or on a standalone switch 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 settings.

spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

no spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

Syntax Description

bpdufilter default	Globally enable BPDU filtering on Port Fast-enabled ports and prevent the switch port connected to end stations from sending or receiving 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(11)AX	This command was first introduced.

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.

Use the **spanning-tree portfast bpdufilter default** global configuration command to globally enable BPDU filtering on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state). The ports still send a few 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 bpdufilter default** global configuration command by using the **spanning-tree bdpufilter** 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 bdpuguard** interface configuration command.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking ports. Configure Port Fast only on ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all ports unless they are individually configured with the **spanning-tree portfast** interface configuration command.

Examples

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking ports:

```
Switch(config)# spanning-tree portfast default
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands**.
spanning-tree bpdufilter	Prevents a port from sending or receiving BPDUs.
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.

spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command on the switch stack or on a standalone switch 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
12.1(11)AX	This command was first introduced.

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 enable Port Fast on a port that is not a trunk port by using the **no spanning-tree portfast** interface configuration command.

The **no spanning-tree portfast** interface configuration command is the same as the **spanning-tree portfast disable** interface configuration command.

Examples

This example shows how to enable the Port Fast feature on an interface on stack member 2:

```
Switch(config)# interface fastethernet2/0/2
Switch(config)# interface gigabitethernet0/2
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 uplinkfast

Use the **spanning-tree uplinkfast** global configuration command on the switch stack or on a standalone switch 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
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **max-update-rate** keyword was added.

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 operating in the rapid-PVST+ or multiple spanning-tree (MST) mode.

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

When you enable or disable UplinkFast, cross-stack UplinkFast (CSUF) also is automatically enabled or disabled on all nonstack port interfaces. CSUF accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.

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 a 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 vlan root primary	Forces this switch to be the root switch.

spanning-tree vlan

Use the **spanning-tree vlan** global configuration command on the switch stack or on a standalone switch to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

spanning-tree vlan *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

Syntax Description

vlan-id	VLAN 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.
forward-time *seconds*	(Optional) 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 *seconds*	(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.
max-age *seconds*	(Optional) 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 *priority*	(Optional) Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that a standalone switch or a switch in the stackthis 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	(Optional) Force this switch to be the root switch.
root secondary	(Optional) Set this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) 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
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The value for the *vlan-id* 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 VLAN does not detect and prevent loops when STP is disabled.

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

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds*, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan** *vlan-id* **root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan** *vlan-id* **root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan** *vlan-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

Examples

This example shows how to disable the STP on VLAN 5:

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

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

This example shows how to set the spanning-tree forwarding time to 18 seconds for 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 instance 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 on the switch stack or on a standalone switch to specify the speed of a 10/100 Mbps or 10/100/1000 Mbps port. Use the **no** or **default** 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 on small form-factor pluggable (SFP) module ports, but you can configure speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation. See "Usage Guidelines" for exceptions when a 1000BASE-T SFP module is in the SFP module port.

Syntax Description

10	Port runs at 10 Mbps.
100	Port runs at 100 Mbps.
1000	Port runs at 1000 Mbps. This option is valid and visible only on 10/100/1000 Mbps-ports.
auto	Port automatically detects the speed it should run at based on the port at the other end of the link.
nonegotiate	Autonegotiation is disabled, and the port runs at 1000 Mbps. This option is valid and visible only on SFP ports. When a 1000BASE-T SFP module is in the SFP module port, the speed can be configured to **10**, **100, 1000**, or **auto**, but not **nonegotiate**.

Defaults

The default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

You can configure the Fast Ethernet port speed as either 10 or 100 Mbps. You can configure the Gigabit Ethernet port speed as 10, 100, or 1000 Mbps. You cannot configure speed on SFP module ports, but you can configure speed to not negotiate (**nonegotiate**) if connected to a device that does not support autonegotiation. However, when a 1000BASE-T SFP module is in the SFP module port, you can configure speed as 10, 100, or 1000 Mbps.

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 ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, do use the **auto** setting on the supported side, but set the duplex and speed on both interfaces.

For 10/100/1000 Mbps ports, if both the speed and duplex are set to specific values, autonegotiation is disabled.

For 10/100 Mbps ports, if both speed and duplex are set to specific values, the link operates at the negotiated speed and duplex value.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

Note For guidelines on setting the switch speed and duplex parameters, refer to the software configuration guide for this release.

Examples

This example shows how to set the specified interface to 100 Mbps:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed 100
```

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

Related Commands

Command	Description
duplex	Specifies the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports.
show interfaces	Displays the statistical information specific to all interfaces or to a specific interface

srr-queue bandwidth limit

Use the **srr-queue bandwidth limit** interface configuration command on the switch stack or on a standalone switch to limit the maximum output on a port. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth limit *weight1*

no srr-queue bandwidth limit

Syntax Description

weight1	Percentage of the port speed to which the port should be limited. The range is 10 to 90.

Defaults

The port is not rate limited and is set to 100 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

If you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed. These values are not exact because the hardware adjusts the line rate in increments of six.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to limit Gigabit Ethernet port 0/1 on stack member 2 to 800 Mbps:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

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

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to the queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue-set.
queue-set	Maps a port to a queue-set.
show mls qos interface queueing	Displays quality of service (QoS) information.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth shape

Use the **srr-queue bandwidth shape** interface configuration command on the switch stack or on a standalone switch to assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth shape *weight1 weight2 weight3 weight4*

no srr-queue bandwidth shape

Syntax Description

weight1 weight2 weight3 weight4	Specify the weights to determine the percentage of the port that is shaped. The inverse ratio (1/*weight*) determines the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.

Defaults

Weight1 is set to 25. Weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

In shaped mode, the queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Use shaping to smooth bursty traffic or to provide a smoother output over time.

The shaped mode overrides the shared mode.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue come into effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to configure the queues for the same port for both shaping and sharing. Because the weight ratios for queues 2, 3, and 4 are set to 0, these queues operate in shared mode. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent. Queue 1 is guaranteed this bandwidth and limited to it; it does not extend its slot to the other queues even if the other queues have no traffic and are idle. Queues 2, 3, and 4 are in shared mode, and the setting for queue 1 is ignored. The bandwidth ratio allocated for the queues in shared mode is 4/(4+4+4), which is 33 percent:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

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

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
priority-queue	Enables the egress expedite queue on an interface.
queue-set	Maps a port to a queue-set.
show mls qos interface queueing	Displays quality of service (QoS) information.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

srr-queue bandwidth share

Use the **srr-queue bandwidth share** interface configuration command on the switch stack or on a standalone switch to assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port. The ratio of the weights is the ratio of frequency in which the shaped round robin (SRR) scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default setting.

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share

Syntax Description

weight1 weight2 weight3 weight4	The ratios of *weight1*, *weight2*, *weight3*, and *weight4* determine the ratio of the frequency in which the SRR scheduler dequeues packets. Separate each value with a space. The range is 1 to 255.

Defaults

Weight1, weight2, weight3, and weight4 are 25 (1/4 of the bandwidth is allocated to each queue).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

The absolute value of each weight is meaningless, and only the ratio of parameters is used.

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among themselves.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in SRR shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue take effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.

Note The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to configure the weight ratio of the SRR scheduler running on egress port Gigabit Ethernet 0/1 on stack member 2. Four queues are used. The bandwidth ratio allocated for each queue in shared mode is 1/(1+2+3+4), 2/(1+2+3+4), 3/(1+2+3+4), and 4/(1+2+3+4), which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

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

Related Commands

Command	Description
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos srr-queue output cos-map	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
priority-queue	Enables the egress expedite queue on an interface.
queue-set	Maps a port to a queue-set.
show mls qos interface queueing	Displays quality of service (QoS) information.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

storm-control

Use the **storm-control** interface configuration command on the switch stack or on a standalone switch to enable broadcast, multicast, or unicast storm control on an interface with the specified threshold level. Use the **no** form of this command to disable broadcast, multicast, or unicast storm control on an interface.

storm-control {**broadcast** | **multicast** | **unicast**} **level** *level* [**.***level*]

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

Syntax Description

broadcast	Enable broadcast storm control on the interface.
multicast	Enable multicast storm control on the interface.
unicast	Enable unicast storm control on the interface.
level	Storm-control suppression level as a percent of total bandwidth. The range is 0 to 100 percent.
.*level*	(Optional) Fractional storm-control suppression level. The range is 0 to 99.

Defaults

Broadcast, multicast, and unicast storm control are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

Storm control is supported only on physical interfaces; it is not supported on EtherChannel port channels, even though it is available in the command-line interface (CLI).

Storm-control suppression level is entered as a percentage of total bandwidth. A threshold value of 100 percent means that no limit is placed on the specified traffic type. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.

When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as Open Shortest Path First (OSPF) and regular multicast data traffic, so both types of traffic are blocked.

Note For more information about storm control suppression levels, refer to the software configuration guide for this release.

Examples

This example shows how to enable multicast storm control with a 75.5 percent threshold level:

```
Switch(config-if)# storm-control multicast level 75.5
```

This example shows how to disable multicast storm control:

```
Switch(config-if)# no storm-control multicast level
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

Related Commands

Command	Description
show storm-control	Displays broadcast, multicast, or unicast storm control settings on all interfaces or on a specified interface.

switch priority

Use the **switch priority** global configuration command on the stack master to change the stack member priority value.

switch *stack-member-number* **priority** *new-priority-value*

Syntax Description

priority *new-priority-value*	Specify the new stack member priority value. The range is 1 to 15.
stack-member-number	Specify the current stack member number. The range 1 to 9.

Defaults

The default priority value is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

If you do not specify a priority value, the default value is assigned.

The new priority value is a factor during a stack-master re-election. Therefore, changing the priority value does not change the stack master immediately.

Use the **reload slot** *current stack member number* privileged EXEC to reset the stack member and apply this configuration change into effect.

Examples

This example shows how to change the priority value of stack member 6 to 9:

```
Switch(config)# switch 6 priority 9
Changing the Switch Priority of Switch Number 6 to 9
Do you want to continue?[confirm]
```

Related Commands

Command	Description
reload	Resets the stack member and puts a configuration change into effect.
session	Accesses a specific stack member.
switch renumber	Changes the stack member number.
show switch	Displays information about the switch stack and its stack members.

switch renumber

Use the **switch renumber** global configuration command on the stack master to change the stack member number.

switch *current-stack-member-number* **renumber** *new-stack-member-number*

Syntax Description

renumber *new-stack-member-number*	Specify the new stack member number for the stack member. The range is 1 to 9.
current-stack-member-number	Specify the current stack member number. The range is 1 to 9.

Defaults

The default stack member number is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

If another stack member is already using the member number that you just specified, the stack master assigns the lowest available number when you reset the stack member.

Note If you change the number of a stack member, and no configuration is associated with the new stack member number, that stack member loses its current configuration and resets to its default configuration. For more information about stack member numbers and configurations, see the software configuration guide.

Use the **reload slot** *current stack member number* privileged EXEC to reset the stack member and apply this configuration change into effect.

Examples

This example shows how to change the member number of stack member 6 to 7:

```
Switch(config)# switch 6 renumber 7
WARNING: Changing the switch number may result in lost
or changed configuration for that switch!
Do you want to continue?[confirm]
```

Related Commands

Command	Description
reload	Resets the stack member and puts a configuration change into effect.
session	Accesses a specific stack member.
switch priority	Changes the stack member priority value.
show switch	Display information about the switch stack and its stack members.

switchport

Use the **switchport** interface configuration command with no keywords on the switch stack or on a standalone switch to put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration. Use the **no** form of this command to put an interface in Layer 3 mode.

switchport

no switchport

Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.

Note If an interface is configured as a Layer 3 interface, you must first enter this **switchport** command with no keywords to configure the interface as a Layer 2 port. Then you can enter additional switchport commands with keywords, as shown on the pages that follow.

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all interfaces are in Layer 2 mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

Entering the **no switchport** command shuts the port down and then re-enables it, which might generate messages on the device to which the port is connected.

Examples

This example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed port.

```
Switch(config-if)# no switchport
```

This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2-switched interface:

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

Note The **switchport** command without keywords is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the switchport status of an interface by entering the **show running-config** 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.
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**.

switchport access

Use the **switchport access** interface configuration command on the switch stack or on a standalone switch to configure a port as a static-access or dynamic-access port. If the switchport mode is set to **access**, the port operates as a member of the specified VLAN. If set to **dynamic**, the port starts discovery of VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access mode to the default VLAN for the switch.

switchport access vlan {*vlan-id* | **dynamic**}

no switchport access vlan

Syntax Description

vlan *vlan-id*	Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094.
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

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

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
12.1(11)AX	This command was first introduced.

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.

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 3750 2970 switches are not VMPS servers. The VMPS server must be configured before a port is configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers (that use bridging protocols) can cause a loss of connectivity.
- Configure the network so that STP does not put the dynamic-access port into an STP blocking state. The Port Fast feature is automatically enabled on dynamic-access ports.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as
  - 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 cause a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN when in access mode:

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

You can verify your setting 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 on the switch stack or on a standalone switch to prevent unknown multicast or unicast packets from being forwarded. Use the **no** form of this command to allow forwarding unknown multicast or unicast packets.

switchport block {**multicast** | **unicast**}

no switchport block {**multicast** | **unicast**}

Syntax Description

multicast	Specify that unknown multicast traffic should be blocked.
unicast	Specify that unknown unicast traffic should be blocked.

Defaults

Unknown multicast and unicast traffic is not blocked.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	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 nonprotected 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
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.

switchport host

Use the **switchport host** interface configuration command on the switch stack or on a standalone switch to optimize a Layer 2 port for a host connection. The **no** form of this command has no affect on the system.

switchport host

Syntax Description

This command has no arguments or keywords.

Defaults

The default is for the port to not be optimized for a host connection.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

To optimize the port for a host connection, the **switchport host** command sets switch port mode to access, enables spanning tree Port Fast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning tree Port Fast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other switches, hubs, concentrators, or bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

Examples

This example shows how to optimize the port configuration for a host connection:

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

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 switchport mode.

switchport mode

Use the **switchport mode** interface configuration command on the switch stack or on a standalone switch 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 {**access**| **dynamic** | **trunk**}

Syntax Description

access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends 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. This is the default switchport mode.
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 sends 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 auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

A configuration that uses the **access** or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to 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.

When 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.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

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.

Access port and trunk ports are mutually exclusive.

The 802.1X feature interacts with switchport modes in these ways:

- If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- If you try to enable 802.1X on a port set to **dynamic auto** or **dynamic desirable**, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to **dynamic auto** or **dynamic desirable**, the port mode is not changed.
- If you try to enable 802.1X on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

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 or dynamic-access port.
switchport trunk	Configures the trunk characteristics when an interface is in trunking mode.

switchport nonegotiate

Use the **switchport nonegotiate** interface configuration command on the switch stack or on a standalone switch 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(11)AX	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: **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.

Examples

This example shows how to cause a port 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 on the switch stack or on a standalone switch to enable port security on the interface. Use the keywords to configure secure MAC addresses, sticky MAC address learning, 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 [**aging**] [**mac-address** *mac-address* [**vlan** *vlan-id*] | **mac-address sticky** [*mac-address*]] [**maximum** *value* [**vlan** *vlan-list*]] [**violation** {**protect** | **restrict** | **shutdown**}]

no switchport port-security [**aging**] [**mac-address** *mac-address* [**vlan** *vlan-id*] | **mac-address sticky** [*mac-address*]] [**maximum** *value* [**vlan** *vlan-list*]] [**violation** {**protect** | **restrict** | **shutdown**}]

Syntax Description

aging	(Optional) See the **switchport port-security aging** command.
mac-address *mac-address*	(Optional) Specify a secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.
vlan *vlan-id*	(Optional) On a trunk port only, specify the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.
mac-address sticky [*mac-address*]	(Optional) Enable the interface for *sticky learning* 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. (Optional) Enter a *mac-address* to specify a sticky secure MAC address.
maximum *value*	(Optional) Set the maximum number of secure MAC addresses for the interface.The maximum number of secure MAC addresses that you can configure on a switch stack is determined by the maximum number of available MAC addresses allowed in the system, approximately 6K. This number is determined by the active Switch Database Management (SDM) template. See the **sdm prefer** command. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces. The default setting is 1.
vlan [*vlan-list*]	(Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the **vlan** keyword is not entered, the default value is used. • **vlan**—set a per-VLAN maximum value. • **vlan** *vlan-list*—set a per-VLAN maximum value on a range of VLANs separated by a hypen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.
violation	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is **shutdown**.

protect	Set the security violation protect mode. In this mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred. **Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.
restrict	Set the security violation restrict mode. In this 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. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
shutdown	Set the security violation shutdown mode. In this mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. 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

The default is to disable port security.

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

The default violation mode is **shutdown**.

Sticky learning is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.
12.1(14)EA1	The **sticky** and **vlan** keywords were added.

Usage Guidelines

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected 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 in the 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 two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP phone, the Cisco IP phone requires up to two MAC addresses. The Cisco IP phone address is learned on the voice VLAN and might also be learned on the access VLAN. Connecting a PC to the Cisco IP phone requires additional MAC addresses.
- 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.

Note Voice VLAN is supported only on access ports and not on trunk ports.

- When a voice VLAN is configured on a secure port that is also configured as a sticky secure port, all addresses on the voice VLAN are learned as dynamic secure addresses, and all addresses seen on the access VLAN to which the port belongs are learned as sticky secure addresses.
- You cannot configure static secure MAC addresses in the voice VLAN.
- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface, or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

If you enable port security on a voice VLAN port and if there is a PC connected to the IP phone, you should set the maximum allowed secure addresses on the port to more than 1.

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.

Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration 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 and adds all sticky secure MAC addresses to the running configuration.

- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky** *mac-address* interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky** *mac-address* interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

Examples

This example shows how to enable port security on Gigabit Ethernet port 12 on stack member 2 and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Switch(config)# interface gigahitethernet 2/0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

This example shows how to configure a secure MAC address and a VLAN ID on Gigabit Ethernet port 12 on stack member 2.

```
Switch(config)# interface gigabitethernet 2/0/12
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

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 using the **show port-security** privileged EXEC command.

Related Commands

Command	Description
show port-security address	Displays all the secure addresses configured on the switch.
show port-security interface *interface-id*	Displays port security configuration for the switch or for the specified interface.

switchport port-security aging

Use the **switchport port-security aging** interface configuration command on the switch stack or on a standalone switch to set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port. Use the **no** form of this command to disable port security aging or to set the parameters to their default states.

switchport port-security aging {**static** | **time** *time* | **type** {**absolute | inactivity**}}

no switchport port-security aging {**static | time | type**}

Syntax Description

static	Enable aging for statically configured secure addresses on this port.
time *time*	Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type	Set the aging type.
absolute	Set absolute aging type. All the secure addresses on this port age out exactly after the time *(*minutes) specified and are removed from the secure address list.
inactivity	Set the inactivity aging type. 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(11)AX	This command was first introduced.

Usage Guidelines

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it become 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 Gigabit Ethernet interface 0/1 on stack member 1.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on Gigabit Ethernet interface 0/2 on stack member 1.

```
Switch(config)# interface gigabitethernet1/0/2
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 on the switch stack or on a standalone switch 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 802.1P priority received from the PC or the attached device with the specified class of service (CoS) value. The range is 0 to 7. Seven is the highest priority. The default is 0.
trust	Set the IP phone port to trust the 802.1P priority received from the PC or the attached device.

Defaults

The default port priority is set to a CoS value of 0 for untagged frames received on the port.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

When voice VLAN is enabled, you can configure the switch to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the switch port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all switch interfaces.)

You should configure voice VLAN on switch access ports. You can only configure a voice VLAN on Layer 2 ports.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the switch by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** 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 on the switch stack or on a standalone switch 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 disable protection on the port.

switchport protected

no switchport protected

Syntax Description

This command has no arguments or keywords.

Defaults

No protected port is defined. All ports are nonprotected.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

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.

Because a switch stack represents a single logical switch, Layer 2 traffic is not forwarded between any protected ports in the switch stack, whether they are on the same or different switches in the stack.

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

Examples

This example shows how to enable a protected port on an interface:

```
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport protected
```

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, including port blocking and port protection settings.
switchport block	Prevents unknown multicast or unicast traffic on the interface.

switchport trunk

Use the **switchport trunk** interface configuration command on the switch stack or on a standalone switch to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

switchport trunk {**allowed vlan** *vlan-list* | **encapsulation** {**dot1q** | **isl** | **negotiate**} | **native vlan** *vlan-id* | **pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan** | **encapsulation** | **native vlan** | {**pruning vlan**}

Syntax Description

allowed vlan *vlan-list*	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 *vlan-list* format. The **none** keyword is not valid. The default is **all**.
encapsulation dot1q	Set the encapsulation format on the trunk port to 802.1Q. With this format, the switch supports simultaneous tagged and untagged traffic on a port.
encapsulation isl	Set the encapsulation format on the trunk port to Inter-Switch Link (ISL). The switch encapsulates all received and sent packets with an ISL header and filters native frames received from an ISL trunk port.
encapsulation negotiate	Specify that if Dynamic Inter-Switch Link (DISL) and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan *vlan-id*	Set the native VLAN for sending and receiving untagged traffic when the interface is in 802.1Q trunking mode. The range is 1 to 4094.
pruning vlan *vlan-list*	Set the list of VLANs that are eligible 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* [**,***vlan-atom...*] where:

- **all** specifies all VLANs from 1 to 4094. 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 VLANs (VLAN IDs greater than 1005) 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; use a hyphen to designate a range of IDs.

- **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 from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **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; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Defaults

The default encapsulation is negotiate.

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(11)AX	This command was first introduced.
12.1(14)EA1	The **allowed vlan** *vlan-list* add, remove, and except keywords were modified to accept the VLAN1 and VLANs 1002 to 1005 values.

Usage Guidelines

Encapsulation:

- The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats.
- You cannot configure one end of the trunk as an 802.1Q trunk and the other end as an ISL or nontrunk port. However, you can configure one port as an ISL trunk and a different port on the same switch as an 802.1Q trunk.
- If you enter the **negotiate** keywords and DTP negotiation does not resolve the encapsulation format, ISL is the selected format. The **no** form of the command resets the trunk encapsulation format to the default.
- The **no** form of the **encapsulation** command resets the encapsulation format to the default.

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.

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. 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.

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.

Examples

This example shows how to cause a port interface configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Switch(config-if)# switchport trunk encapsulation dot1q
```

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, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport voice vlan

Use the **switchport voice vlan** interface configuration command on the switch stack or on a standalone switch 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

vlan-id	Specify the VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an 802.1Q priority of 5.
dot1p	Configure the telephone to use 802.1P 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	Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
untagged	Configure the telephone to send untagged voice traffic. This is the default for the telephone.

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(11)AX	This command was first introduced.

Usage Guidelines

You should configure voice VLAN on Layer 2 access ports.

You must enable Cisco Discovery Protocol (CDP) on the switchport connected to the Cisco IP phone for the switch to send configuration information to the phone. CDP is enabled by default globally and on the interface.

Before you enable voice VLAN, we recommend you enable quality of service (QoS) on the switch by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** interface configuration command.

When you enter a VLAN ID, the IP phone forwards voice traffic in 802.1Q frames, tagged with the specified VLAN ID. The switch puts 802.1Q voice traffic in the voice VLAN.

When you select **dot1q**, **none**, or **untagged**, the switch puts the indicated voice traffic in the access VLAN.

In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

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. When the port is connected to a Cisco IP phone, the IP phone requires two MAC addresses: one for the access VLAN and the other for the voice VLAN. Connecting a PC to the IP phone requires additional MAC addresses.

If any type of port security is enabled on the access VALN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

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 *interface-id* **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** global configuration command on the switch stack or on a standalone switch to set the maximum packet size or maximum transmission unit (MTU) size for Gigabit Ethernet ports or for Fast Ethernet (10/100) ports. Use the **no** form of this command to restore the global MTU value to its default value.

system mtu {*bytes* | **jumbo** *bytes*}

no system mtu

Syntax Description

bytes	Set the system MTU for Fast Ethernet (10/100) portsports set to 10 or 100 Mbps. The range is 1500 to 1546 bytes.
jumbo *bytes*	Set the system jumbo frame size (MTU) for Gigabit Ethernet ports. The range is 1500 to 9000 bytes.

Defaults

The default MTU size for all ports is 1500 bytes.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)AX	This command was first introduced.

Usage Guidelines

When you use this command to change the MTU size, you must reset the switch before the new configuration takes effect.

Gigabit Ethernet ports are not affected by the **system mtu** command; Fast Ethernet 10/100 Mbps ports are not affected by the **system mtu jumbo** command.

If you enter a value that is outside the range for the specific type of switch, the value is not accepted.

Note The switch does not support setting the MTU on a per-interface basis.

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, SNMP, Telnet, or routing protocols.

Examples

This example shows how to set the maximum packet size for Gigabit Ethernet ports to 1800 bytes:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

You can verify your setting by entering the **show system mtu** privileged EXEC command.

Related Commands

Command	Description
show system mtu	Displays the packet size set for 10/100 Fast Ethernet and Gigabit Ethernet ports.

test cable-diagnostics tdr

Use the **test cable-diagnostics tdr** privileged EXEC command on the switch stack or on a standalone switch to run the Time Domain Reflector (TDR) feature on an interface.

test cable-diagnostics tdr interface *interface-id*

Syntax Description

interface-id	Specify the interface on which to run TDR.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

You can use the TDR feature to diagnose and resolve cabling problems. TDR is supported only on copper Ethernet 10/100/1000 ports. It is not supported on 10/100 ports or small form-factor pluggable (SFP) module ports. For more information about TDR, refer to the software configuration guide for this release.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

Examples

This example shows how to run TDR on an interface:

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has a link staus of up and a speed of 10 or 100 Mbps, these messages appear:

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/9
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/9
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

Related Commands

Command	Description
show cable-diagnostics tdr	Displays the TDR results.