

# 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		
<i>index</i>		Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535.
<b>owner name</b>		(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
	<b>show rmon statistics</b>	Displays RMON statistics.  For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS System Management Commands &gt; RMON Commands</b> .

# 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. Use the **no** form of this command to return to the default template.

**sdm prefer {routing | vlan}**

**no sdm prefer**

Syntax Description	routing	vlan
	Provide maximum system utilization for unicast routing. You would typically use this template for a router or aggregator in the middle of a network.	Provide maximum system utilization for VLANs. This template maximizes system resources for use as a Layer 2 switch with no routing.

**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.

**Usage Guidelines** You must reload the switch for the configuration to take effect.

All stack members use the same SDM 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.

Use the **sdm prefer vlan** 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** global configuration command prevents other features from using the memory allocated to unicast routing in the routing template (approximately 11 K).

Table 2-12 lists the approximate number of each resource supported in each of the three templates for a switch. The first seven 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 two rows, the total number of routed ports and SVIs and the number of Layer 2 VLANs, are guidelines used to calculate hardware resource consumption related to the other resource parameters.

**Table 2-12 Approximate Number of Feature Resources Allowed by Each Template**

Resource	Default Template	Routing Template	VLAN Template
Unicast MAC addresses	6 K	3 K	12 K
IGMP groups and multicast routes	1 K	1 K	1 K
Unicast routes	8 K	11 K	0
• Directly connected hosts	6 K	3 K	0
• Indirect routes	2 K	8 K	0
QoS classification ACEs	512	512	512
Security ACEs	1 K	1 K	1 K
Routed interfaces (routed ports and SVIs)	8	8	8
Layer 2 VLANs	1 K	1 K	1 K

The total number of routed interfaces is not limited by software and can be set to a number higher than shown in the tables. If the number of routed interfaces configured is lower or equal to the number in the tables, the number of entries in each category (Unicast MAC addresses, IGMP groups, and so on) for each template will be as shown. As the number of routed interfaces is increased, CPU utilization typically increases. If the number of routed interfaces is increased beyond the number shown in the tables, the number of supported entries in each category could decrease depending on other features that are enabled.

### Examples

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

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

This example shows how to remove the routing template and to use the default template:

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

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

### Related Commands

Command	Description
<a href="#">show sdm prefer</a>	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 a 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 default action is for the password-recovery mechanism to be 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 defaults. Do not keep a backup copy of the config file on the switch.

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

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

**Examples**

This example shows how to disable password recovery on a switch 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
<a href="#">show version</a>	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
	<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
	<a href="#">show policy-map</a>	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*

<b>Syntax Description</b>	<i>stack-member-number</i>	Specify the current stack member number. The stack member number is in the range from 1 through 9.
---------------------------	----------------------------	--

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

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

<b>Usage Guidelines</b>	When you access the stack member, its stack member number is appended to the system prompt.
-------------------------	---

<b>Examples</b>	This example shows how to access stack member 6:
-----------------	--

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

Related Commands	Command	Description
	<a href="#">reload</a>	Saves the configuration change and restarts the stack member.
	<a href="#">switch priority</a>	Changes the stack member priority value.
	<a href="#">switch renumber</a>	Changes the stack member number.
	<a href="#">show switch</a>	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

<b>ip dscp</b> <i>new-dscp</i>	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.
<b>ip precedence</b> <i>new-precedence</i>	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 same as 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
<b>class</b>	Defines a traffic classification match criteria (through the <b>police</b> , <b>set</b> , and <b>trust</b> policy-map class configuration commands) for the specified class-map name.
<b>police</b>	Defines a policer for classified traffic.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
<b>show policy-map</b>	Displays quality of service (QoS) policy maps.
<b>trust</b>	Defines a trust state for traffic classified through the <b>class</b> policy-map configuration command or the <b>class-map</b> 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$0XclwyT.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
<b>show running-config</b>	Displays the running configuration on the switch. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
<a href="#">show version</a>	Displays version information for the hardware and firmware.

# 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] [ | {begin | exclude | include} expression]
```

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



## Note

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

**Command Modes** Privileged EXEC

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

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

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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 2-13](#) describes each field in the display.

```
Switch# show boot
BOOT path-list:      flash:c3750-i5q3l2-mz-121.11.AX/c3750-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:
NVRAM/Config file
  buffer size:      32768
```

**Table 2-13** show boot Field Descriptions

Field	Description
BOOT path-list	<p>Displays a semicolon separated list of executable files to try to load and execute when automatically booting.</p> <p>If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the Flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.</p> <p>If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the Flash file system.</p>
Config file	Displays the filename that 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.
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
<b>boot config-file</b>	Specifies the filename that IOS uses to read and write a nonvolatile copy of the system configuration.
<b>boot enable-break</b>	Enables interrupting the automatic boot process.
<b>boot manual</b>	Enables manually booting the switch during the next boot cycle.
<b>boot private-config-file</b>	Specifies the filename that IOS uses to read and write a nonvolatile copy of the private configuration.
<b>boot system</b>	Specifies the IOS image to load during the next boot cycle.

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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
	<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
	<a href="#">match (class-map configuration)</a>	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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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
<a href="#">cluster enable</a>	Enables a command-capable switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it.
<a href="#">show cluster candidates</a>	Displays a list of candidate switches.
<a href="#">show cluster members</a>	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		
<b>detail</b>	(Optional)	Display detailed information for all candidates.
<b>mac-address</b> <i>H.H.H.</i>	(Optional)	MAC address of the cluster candidate.
<b>begin</b>	(Optional)	Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional)	Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional)	Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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-C3750-12T 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-C3750-12T
  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
<a href="#">show cluster</a>	Displays the cluster status and a summary of the cluster to which the switch belongs.
<a href="#">show cluster members</a>	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	
<i>n</i>	(Optional) Number that identifies a cluster member. The range is 0 to 15.
<b>detail</b>	(Optional) Display detailed information for all cluster members.
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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

SN MAC Address      Name           PortIf  FEC Hops  |---Upstream---|
0  0002.4b29.2e00  StLouis1      0        0
1  0030.946c.d740  tal-switch-1  Fa0/13   1    0  Gi0/1      Up   (Cmdr)
2  0002.b922.7180  nms-2820     10       0    2    1  Fa0/18     Up
3  0002.4b29.4400  SanJuan2     Gi0/1    2    1    1  Fa0/11     Up
4  0002.4b28.c480  GenieTest    Gi0/2    2    1    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-C3750-12T
  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-C3750-12T
  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-C3750-12T
  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
<a href="#">show cluster</a>	Displays the cluster status and a summary of the cluster to which the switch belongs.
<a href="#">show cluster candidates</a>	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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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
<a href="#">show controllers ethernet-controller</a>	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.
<a href="#">show interfaces</a>	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

<i>interface-id</i>	The physical interface (including type, stack member, module, and port number).
<b>phy</b>	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the device or the interface.
<b>detail</b>	(Optional) Display details about the PHY internal registers.
<b>port-asic</b>	(Optional) Display information about the port ASIC internal registers.
<b>configuration</b>	Display port ASIC internal register configuration.
<b>statistics</b>	Display port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(11)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:

```
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 8 collision frames                    0 Minimum size frames
  0 9 collision frames                    0 65 to 127 byte frames
  0 10 collision frames                   0 128 to 255 byte frames
  0 11 collision frames                   0 256 to 511 byte frames
  0 12 collision frames                   0 512 to 1023 byte frames
  0 13 collision frames                   0 1024 to 1518 byte frames
  0 14 collision frames
  0 15 collision frames
  0 Excessive collisions
  0 Late collisions                       0 Overrun frames
  0 VLAN discard frames                   0 Pause frames
  0 Excess defer frames                   0 Symbol error frames
  0 64 byte frames
  0 127 byte frames
  0 255 byte frames
  0 511 byte frames
  0 1023 byte frames
  0 1518 byte frames
  0 Too large frames
  0 Good (1 coll) frames

```

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

```
Switch# show controllers ethernet-controller phy
```

```
GigabitEthernet1/0/1 (gpn: 3, port-number: 1)
```

```

-----
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 Register : 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 0011 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 1110 0000
Receive Error Counter     : 0000 0000 0000 0000

```

### show controllers ethernet-controller

```

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 0000 1010
Disable Receiver 1     : 0000 0000 0000 00GigabitEthernet1/0/2 (gpn: 4,
port-number: 2)

```

```

-----
Control Register       : 0011 0001 0000 0000
Control STATUS        : 0111 1000 0000 1001
Phy ID 1              : 0000 0000 0001 0011
Phy ID 2              : 0111 1000 1111 1011
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
Auto-Negotiation Expansion Reg : 0000 0000 0000 0100

```

<output truncated>

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 0000FF8 00000000
                        0000088A 0000085D 0000FF8 00000000
TransmitRingFifoInfo    : 00000016 00000016 40000000 00000000
                        0000000C 0000000C 40000000 00000000
TransmitBufferInfo      : 00012000 0000FFF 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

```

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
<a href="#">show boot</a>	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
<a href="#">show controllers tcam</a>	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 [detail] [ | {begin | exclude | include} expression]
```

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

**Command Modes** 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 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
<a href="#">show controllers cpu-interface</a>	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
<a href="#">show controllers ethernet-controller</a>	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 [interface interface-id | statistics [interface interface-id]] [ | {begin | exclude | include} expression]
```

## Syntax Description

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

## Command Modes

Privileged EXEC

## Command History

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

## 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.

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

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

## Examples

This is an example of output from the **show dot1x** privileged EXEC command:

```
Switch# show dot1x

Global 802.1X Parameters
reauth-enabled          yes
reauth-period           3600
quiet-period            60
tx-period               30
supp-timeout            30
server-timeout          30
reauth-max              2
max-req                 2
```

```

802.1X Port Summary
Port Name           Status   Mode           Authorized
Gi1/0/1             disabled n/a            n/a
Gi1/0/2             enabled  Auto (negotiate) yes
Gi1/0/3             disabled n/a            n/a
Gi1/0/4             disabled n/a            n/a
<output truncated>

Gi2/0/1             disabled n/a            n/a
Gi2/0/2             disabled n/a            n/a
Gi2/0/3             enabled  Auto (negotiate) yes

<output truncated>

802.1X Port Details
802.1X is disabled on GigabitEthernet1/0/1

802.1X is enabled on GigabitEthernet1/0/2
Status              Unauthorized
Port-control        Auto
Supplicant          0060.b0f8.fbf8
Multiple Hosts      Disallowed
Current Identifier   2

Authenticator State Machine
State               AUTHENTICATING
Reauth Count        1

Backend State Machine
State               RESPONSE
Request Count       0
Identifier (Server) 2

Reauthentication State Machine
State               INITIALIZE

802.1X is disabled on GigabitEthernet1/0/3

802.1X is disabled on GigabitEthernet1/0/4

<output truncated>

```

**Note**

In the previous display, the `supp-timeout`, `server-timeout`, and `reauth-max` values in the Global 802.1X Parameters section are not configurable. When relaying a request from the RADIUS authentication server to the client, the `supp-timeout` is the amount of time the switch waits for a response before it resends the request. When relaying a response from the client to the RADIUS authentication server, the `server-timeout` is the amount of time the switch waits for a reply before it resends the response. The `reauth-max` parameter is the maximum number of times that the switch tries to authenticate the client without receiving any response before the switch resets the port and restarts the authentication process.

In the 802.1X Port Summary section of the display, the Status column shows whether the port is enabled for 802.1X (the `dot1x port-control` interface configuration command is set to `auto` or `force-unauthorized`). The Mode column shows the operational status of the port. For example, if you configure the `dot1x port-control` interface configuration command to `force-unauthorized`, but the port has not transitioned to that state, the Mode column displays `auto`. If you disable 802.1X, the Mode column displays `n/a`.

The Authorized column shows the authorization state of the port. For information about port states, refer to the “Configuring 802.1X Port-Based Authentication” chapter in the software configuration guide for this release.

This is an example of output from the **show dot1x interface gigabitethernet1/0/2** privileged EXEC command. Table 2-14 describes the fields in the display.

```
Switch# show dot1x interface gigabitethernet1/0/2

802.1X is enabled on GigabitEthernet1/0/2
  Status                Authorized
  Port-control          Auto
  Supplicant            0060.b0f8.fbf8
  Multiple Hosts        Disallowed
  Current Identifier    3

  Authenticator State Machine
    State                AUTHENTICATED
    Reauth Count        0

  Backend State Machine
    State                IDLE
    Request Count        0
    Identifier (Server)  2

  Reauthentication State Machine
    State                INITIALIZE
```

**Table 2-14** show dot1x interface Field Description

Field	Description
<b>802.1X is enabled on GigabitEthernet1/0/2</b>	
Status	Status of the port (authorized or unauthorized). The status of a port is displayed as authorized if the <b>dot1x port-control</b> interface configuration command is set to <b>auto</b> and has successfully completed authentication.
Port-control	Setting of the <b>dot1x port-control</b> interface configuration command.
Supplicant	Ethernet MAC address of the client, if one exists. If the switch has not discovered the client, this field displays <i>Not set</i> .
Multiple Hosts	Setting of the <b>dot1x multiple-hosts</b> interface configuration command (allowed or disallowed).
Current Identifier <sup>1</sup>	Each exchange between the switch and the client includes an identifier, which matches requests with responses. This number is incremented with each exchange and can be reset by the authentication server.

1. This field and the remaining fields in the display show internal state information. For a detailed description of these state machines and their settings, refer to the IEEE 802.1X specification.

This is an example of output from the **show dot1x statistics interface gigabitethernet2/0/3** command. [Table 2-15](#) describes the fields in the display.

```
Switch# show dot1x statistics interface gigabitethernet2/0/3

GigabitEthernet2/0/3

Rx:  EAPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
     Start      Logoff     Invalid    Total      Resp/Id   Resp/Oth  LenError
     0          0          0          21         0         0         0

     Last      Last
     EAPOLVer  EAPOLSrc
     1         0002.4b29.2a03

Tx:  EAPOL      EAP      EAP
     Total      Req/Id   Req/Oth
     622        445     0
```

**Table 2-15** show dot1x statistics Field Descriptions

Field	Description
RX EAPOL Start	Number of valid EAPOL-start frames that have been received
RX EAPOL Logoff	Number of EAPOL-logoff frames that have been received
RX EAPOL Invalid	Number of EAPOL frames that have been received and have an unrecognized frame type
RX EAPOL Total	Number of valid EAPOL frames of any type that have been received
RX EAP Resp/ID	Number of EAP-response/identity frames that have been received
RX EAP Resp/Oth	Number of valid EAP-response frames (other than response/identity frames) that have been received
RX EAP LenError	Number of EAPOL frames that have been received in which the packet body length field is invalid
Last EAPOLVer	Protocol version number carried in the most recently received EAPOL frame
LAST EAPOLSrc	Source MAC address carried in the most recently received EAPOL frame
TX EAPOL Total	Number of EAPOL frames of any type that have been sent
TX EAP Req/Id	Number of EAP-request/identity frames that have been sent
TX EAP Req/Oth	Number of EAP-request frames (other than request/identity frames) that have been sent

#### Related Commands

Command	Description
<a href="#">dot1x default</a>	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

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

## Command Modes

User EXEC

## Command History

Release	Modification
12.1(11)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**

<b>Command</b>	<b>Description</b>
<b>show interfaces trunk</b>	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		
<b>all</b>		Display both fan and temperature environmental status.
<b>fan</b>		Display the switch fan status.
<b>power</b>		Display the switch power status.
<b>rps</b>		Display whether an RPS 300 Redundant Power System is connected to the switch.
<b>stack</b> [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.
<b>temperature</b>		Display the switch temperature status.
<b>begin</b>	(Optional)	Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional)	Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional)	Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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 issued 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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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.

On the Catalyst 3750 switch, a displayed gbic-invalid error reason refers to an invalid small form-factor pluggable (SFP) interface.

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

```
Switch> show errdisable detect
ErrDisable Reason    Detection status
-----
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
gbic-invalid         Enabled
```

Related Commands	Command	Description
	<a href="#">errdisable detect cause</a>	Enables error-disable detection for a specific cause or all causes.
	<a href="#">show errdisable flap-values</a>	Displays error condition recognition information.
	<a href="#">show errdisable recovery</a>	Displays error-disable recovery timer information.
	<a href="#">show interfaces status</a>	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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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
	<a href="#">errdisable detect cause</a>	Enables error-disable detection for a specific cause or all causes.
	<a href="#">show errdisable detect</a>	Displays error-disable detection status.
	<a href="#">show errdisable recovery</a>	Displays error-disable recovery timer information.
	<a href="#">show interfaces status</a>	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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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.

On the Catalyst 3750 switch, 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
channel-misconfig      Disabled
vmps                   Disabled
pagp-flap              Disabled
dtp-flap               Disabled
link-flap              Disabled
psecure-violation      Disabled
gbic-invalid           Disabled
loopback               Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

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

## ■ show errdisable recovery

Related Commands	Command	Description
	<a href="#">errdisable recovery</a>	Configures the recover mechanism variables.
	<a href="#">show errdisable detect</a>	Displays error disable detection status.
	<a href="#">show errdisable flap-values</a>	Displays error condition recognition information.
	<a href="#">show interfaces status</a>	Displays interface status or a list of interfaces in error-disabled state.

# show etherchannel

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

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

Syntax Description	
<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 12.
<b>brief</b>	Display a summary of EtherChannel information.
<b>detail</b>	Display detailed EtherChannel information.
<b>load-balance</b>	Display the load-balance or frame-distribution scheme among ports in the port channel.
<b>port</b>	Display EtherChannel port information.
<b>port-channel</b>	Display port-channel information.
<b>summary</b>	Display a one-line summary per channel-group.
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	
	User EXEC

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

**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 = 8
Port-channels: 1 Max Port-channels = 1
              Ports in the group:
              -----
Port: Gi1/0/1
-----
```

## show etherchannel

```

Port state      = Up Mstr In-Bndl
Channel group = 1          Mode = Desirable-S1      Gcchange = 0
Port-channel   = Po1      GC   = 0x00010001      Pseudo port-channel = Po1
Port index     = 0          Load = 0x00

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

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

Local information:

Port      Flags State  Timers  Hello  Partner  PAgP    Learning  Group
Gi1/0/1   SC   U6/S7  H       30s   1        128     Any       16

Partner's information:

Port      Partner      Partner      Partner      Partner Group
Name      Device ID    Port         Age  Flags  Cap.
Gi0/1     vegas-p2    0002.4b29.4600  Gi0/1     9s SC  10001

Age of the port in the current state: 00d:00h:07m:52s
Port: Gi1/0/2
-----

Port state      = Up Mstr In-Bndl
Channel group = 1          Mode = Desirable-S1      Gcchange = 0
Port-channel   = Po1      GC   = 0x00010001      Pseudo port-channel = Po1
Port index     = 0          Load = 0x00

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

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

Local information:

Port      Flags State  Timers  Hello  Partner  PAgP    Learning  Group
Gi1/0/2   SC   U6/S7  H       30s   1        128     Any       16

Partner's information:

Port      Partner      Partner      Partner      Partner Group
Name      Device ID    Port         Age  Flags  Cap.
Gi0/2     vegas-p2    0002.4b29.4600  Gi0/2     4s SC  10001

Age of the port in the current state: 00d:00h:07m:55s

Port-channels in the group:
-----
Port-channel: Po1
-----

Age of the Port-channel = 00d:00h:08m:28s
Logical slot/port      = 1/0          Number of ports = 2
GC                     = 0x00010001      HotStandBy port = null
Port state             = Port-channel Ag-Inuse

Ports in the Port-channel:

Index  Load  Port      EC state
-----+-----+-----+-----

```

```

0      00      Gi1/0/1      desirable-sl
0      00      Gi1/0/2      desirable-sl

Time since last port bundled:    00d:00h:07m:56s    Gi1/0/1

```

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

```

Switch> show etherchannel 1 summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       R - Layer3        S - Layer2
       U - port-channel in use
Group Port-channel  Ports
-----+-----+-----
1      Po1(SU)      Gi1/0/1(P)  Gi1/0/2(P)

```

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

```

Switch> show etherchannel 1 brief
Group state = L2
Ports: 2    Maxports = 8
Port-channels: 1 Max Port-channels = 1

```

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
-----

Age of the Port-channel    = 00d:00h:10m:41s
Logical slot/port          = 1/0              Number of ports = 2
GC                          = 0x00010001      HotStandBy port = null
Port state                  = Port-channel Ag-Inuse

Ports in the Port-channel:

Index  Load  Port      EC state
-----+-----+-----
0      00    Gi1/0/1   desirable-sl
0      00    Gi1/0/2   desirable-sl

Time since last port bundled:    00d:00h:10m:08s    Gi1/0/1

```

### Related Commands

Command	Description
<a href="#">channel-group</a>	Assigns an Ethernet interface to an EtherChannel group.
<a href="#">interface port-channel</a>	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 | counters | description | etherchannel |
flowcontrol | pruning | stats | status [err-disabled] | switchport | trunk] [ | { begin | exclude
| include } expression]
```

## Syntax Description

<i>interface-id</i>	(Optional) Valid interfaces include physical ports (including type, stack member, module, and port number) and port channels. The valid port-channel range is 1 to 12.
<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN identification. The range is 1 to 4094.
<b>accounting</b>	(Optional) Display accounting information on the interface, including active protocols and input and output packets and octets.
<b>counters</b>	(Optional) See the <a href="#">show interfaces counters</a> command.
<b>description</b>	(Optional) Display the administrative status and description set for an interface.
<b>etherchannel</b>	(Optional) Display interface EtherChannel information.
<b>flowcontrol</b>	(Optional) Display interface flowcontrol information
<b>pruning</b>	(Optional) Display interface trunk VTP pruning information.
<b>stats</b>	(Optional) Display the input and output packets by switching path for the interface.
<b>status</b>	(Optional) Display the status of the interface.
<b>err-disabled</b>	(Optional) Display interfaces in error-disabled state.
<b>switchport</b>	(Optional) Display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
<b>trunk</b>	Display interface trunk information. If you do not specify an interface, information for only active trunking ports is displayed.
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



## Note

Though visible in the command-line help strings, the **capabilities**, **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.

**Usage Guidelines**

Expressions are case sensitive. For example, if you enter **l 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 gigabitethernet 3/0/3
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 gigabitethernet 1/0/4 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
```

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 gigabitethernet1/0/6 pruning
Port  Vlans pruned for lack of request by neighbor
Gi1/0/6  3,4

Port  Vlans traffic requested of neighbor
Gi1/0/6  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
```

<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
```

This is an example of output from the **show interfaces switchport** command for a single interface. [Table 2-16](#) describes the fields in the display.

**Note**

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

```
Switch# show interfaces gigabitethernet 1/0/3 switchport
Name: Gi1/0/3
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

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

**Table 2-16** *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.
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.

**Table 2-16 show interfaces switchport Field Descriptions (continued)**

Field	Description
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 fastethernet 1/0/47 trunk

Port      Mode      Encapsulation  Status      Native vlan
Fa1/0/47  desirable n-isl          trunking    1

Port      Vlans allowed on trunk
Fa1/0/47  1-4094

Port      Vlans allowed and active in management domain
Fa1/0/47  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
Fa1/0/47  1-4,20,34-36,38-55,57-58,66-67,100,139,200-201,1000
```

**Related Commands**

Command	Description
<a href="#">switchport access</a>	Configures a port as a static-access or dynamic-access port.
<a href="#">switchport block</a>	Blocks unknown unicast or multicast traffic on an interface.
<a href="#">switchport mode</a>	Configures the VLAN membership mode of a port.
<a href="#">switchport protected</a>	Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch.
<a href="#">switchport trunk pruning</a>	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		
<i>interface-id</i>	(Optional) ID of the physical interface, including type, stack member, module, and port number.	
<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN number of the management VLAN. The range is 1 to 4094.	
<b>broadcast</b>	(Optional) Display discarded broadcast traffic.	
<b>errors</b>	(Optional) Display error counters.	
<b>module</b> <i>switch-number</i>	(Optional) Display counters for the specified stack member. The range is from 1 to 9, depending upon the switch numbers in the stack.	
	<b>Note</b> In this command, the <b>module</b> keyword refers to the stack member number (1–9). In other commands that contain an interface ID, the <b>module</b> number is always zero.	
<b>multicast</b>	(Optional) Display discarded multicast traffic.	
<b>trunk</b>	(Optional) Display trunk counters.	
<b>unicast</b>	(Optional) Display discarded unicast traffic.	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .	
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .	
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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
```

<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
```

<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
```

```
Fal/0/3          80678          4155          0
Fal/0/4          82320          126           0
Fal/0/5          0              0             0
```

<output truncated>

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show interfaces</a>	Displays additional interface characteristics.
<a href="#">show storm-control</a>	Displays storm-control settings for an interface or all interfaces.
<a href="#">storm-control</a>	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

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

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(11)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
<a href="#">ip igmp profile</a>	Configures the specified IGMP profile number.

# show ip igmp snooping

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

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

Syntax Description	
<b>mrouter</b>	(Optional) See the <a href="#">show ip igmp snooping mrouter</a> command.
<b>multicast</b>	(Optional) See the <a href="#">show ip igmp snooping multicast</a> command.
<b>vlan <i>vlan-id</i></b>	(Optional) Specify a VLAN; the range is 1 to 4094.
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Use this command to display snooping configuration for the switch or for a specific VLAN. Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

**Examples** This is an example of output from the **show ip igmp snooping** command. It shows how to display snooping characteristics for all VLANs on the switch.

```
Switch# show ip igmp snooping
vlan 1
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
vlan 2
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
<output truncated>
```

## ■ show ip igmp snooping

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

```
Switch# show ip igmp snooping vlan 1
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
```

### Related Commands

Command	Description
<a href="#">ip igmp snooping</a>	Enables and configures IGMP snooping on the switch or on a VLAN.
<a href="#">show ip igmp snooping mrouter</a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN
<a href="#">show ip igmp snooping multicast</a>	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		
<b>vlan</b> <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 4094.	
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .	
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .	
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12/1(11)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
	<a href="#">ip igmp snooping</a>	Enables and configures IGMP snooping on the switch or on a VLAN.
	<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN
	<a href="#">show ip igmp snooping multicast</a>	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

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

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(11)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       224.1.1.2.30      IGMP     Fa3/0/31, Fa4/0/1
1       224.1.1.2.1       IGMP     Fa3/0/31, Fa4/0/1
1       224.4.4.4         USER     Fa1/0/4, Fa4/0/1
```

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
1         224.1.2.1          IGMP     Fa4/0/1, Fa4/0/37
```

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
```

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
1         224.1.2.1          IGMP     Fa4/0/1, Fa4/0/37
```

## Related Commands

Command	Description
<a href="#">ip igmp snooping</a>	Enables and configures IGMP snooping on the switch or on a VLAN.
<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN.
<a href="#">show ip igmp snooping mrouter</a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

# 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]
```

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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 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
	<b>clear mac-address-table dynamic</b>	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.
	<b>show mac-address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
	<b>show mac-address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<b>show mac-address-table dynamic</b>	Displays dynamic MAC address table entries only.
	<b>show mac-address-table interface</b>	Displays the MAC address table information for the specified interface.
	<b>show mac-address-table multicast</b>	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
	<b>show mac-address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<b>show mac-address-table static</b>	Displays static MAC address table entries only.
	<b>show mac-address-table vlan</b>	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]
```

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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 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**

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

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

**Command Modes** User EXEC

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

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

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

**Command Modes** User EXEC

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

**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**

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

## Syntax Description

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

## Command Modes

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

## 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 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**

<b>Command</b>	<b>Description</b>
<b>clear mac-address-table dynamic</b>	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.
<b>show mac-address-table address</b>	Displays MAC address table information for the specified MAC address.
<b>show mac-address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
<b>show mac-address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
<b>show mac-address-table interface</b>	Displays the MAC address table information for the specified interface.
<b>show mac-address-table multicast</b>	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
<b>show mac-address-table static</b>	Displays static MAC address table entries only.
<b>show mac-address-table vlan</b>	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]
```

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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 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**

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

## Syntax Description

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



## Note

Though visible in the command-line help string, 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.

## 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
<a href="#">show mac-address-table address</a>	Displays MAC address table information for the specified MAC address.
<a href="#">show mac-address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
<a href="#">show mac-address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
<a href="#">show mac-address-table dynamic</a>	Displays dynamic MAC address table entries only.
<a href="#">show mac-address-table interface</a>	Displays the MAC address table information for the specified interface.
<a href="#">show mac-address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.
<a href="#">show mac-address-table static</a>	Displays static MAC address table entries only.
<a href="#">show mac-address-table vlan</a>	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]
```

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

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(8)AX	This command was first introduced.

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

## Syntax Description

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

## 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
----    -
A11     0100.0ccc.cccc  STATIC  CPU
A11     0180.c200.0000  STATIC  CPU
A11     0100.0ccc.cccd  STATIC  CPU
A11     0180.c200.0001  STATIC  CPU
A11     0180.c200.0002  STATIC  CPU
A11     0180.c200.0003  STATIC  CPU
A11     0180.c200.0004  STATIC  CPU
A11     0180.c200.0005  STATIC  CPU
A11     0180.c200.0006  STATIC  CPU
A11     0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 10
```

Related Commands	Command	Description
	<b>mac-address-table static</b>	Adds static addresses to the MAC address table.
	<b>show mac-address-table address</b>	Displays MAC address table information for the specified MAC address.
	<b>show mac-address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
	<b>show mac-address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<b>show mac-address-table dynamic</b>	Displays dynamic MAC address table entries only.
	<b>show mac-address-table interface</b>	Displays the MAC address table information for the specified interface.
	<b>show mac-address-table multicast</b>	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
	<b>show mac-address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<b>show mac-address-table vlan</b>	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 ]
```

## Syntax Description

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

## Command Modes

User EXEC

## Command History

Release	Modification
12.1(11)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 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
	<b>show mac-address-table address</b>	Displays MAC address table information for the specified MAC address.
	<b>show mac-address-table aging-time</b>	Displays the aging time in all VLANs or the specified VLAN.
	<b>show mac-address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<b>show mac-address-table dynamic</b>	Displays dynamic MAC address table entries only.
	<b>show mac-address-table interface</b>	Displays the MAC address table information for the specified interface.
	<b>show mac-address-table multicast</b>	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
	<b>show mac-address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<b>show mac-address-table static</b>	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		
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .	
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .	
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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
	<a href="#">mls qos</a>	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

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

## Command Modes

User EXEC

## Command History

Release	Modification
12.1(11)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
<a href="#">mls qos aggregate-policer</a>	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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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**

<b>Command</b>	<b>Description</b>
<a href="#">mls qos srr-queue input bandwidth</a>	Assigns shaped round robin (SRR) weights to an ingress queue.
<a href="#">mls qos srr-queue input buffers</a>	Allocates the buffers between the ingress queues.
<a href="#">mls qos srr-queue input cos-map</a>	Maps assigned class of service (CoS) values to an ingress queue and assigns CoS values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue input dscp-map</a>	Maps assigned Differentiated Services Code Point (DSCP) values to an ingress queue and assigns DSCP values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue input priority-queue</a>	Configures the ingress priority queue and guarantees bandwidth.
<a href="#">mls qos srr-queue input threshold</a>	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

<i>interface-id</i>	(Optional) Display QoS information for the specified interface. Valid interfaces include physical ports.
<b>buffers</b>	(Optional) Display the buffer allocation among the queues.
<b>queueing</b>	(Optional) Display the queueing strategy (shared or shaped) and the weights corresponding to the queues.
<b>statistics</b>	(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.
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



## Note

Though visible in the command-line help string, 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
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 buffers** command:

```
Switch> show mls qos interface fastethernet1/0/7 buffers
FastEthernet1/0/7
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 queuing** command:

```
Switch> show mls qos interface fastethernet1/0/7 queuing
FastEthernet1/0/7
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 statistics** command.

[Table 2-17](#) describes the fields in this display.

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

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      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      0

cos: incoming
-----
 0 - 4 :    132067      0      0      0      0
 5 - 9 :         0      0      0
```

## ■ show mls qos interface

```

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

Policer: Inprofile:      0 OutofProfile:      0

```

**Table 2-17** 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
	<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to a queue-set.
	<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
	<a href="#">mls qos srr-queue input bandwidth</a>	Assigns shaped round robin (SRR) weights to an ingress queue.
	<a href="#">mls qos srr-queue input buffers</a>	Allocates the buffers between the ingress queues.
	<a href="#">mls qos srr-queue input cos-map</a>	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
	<a href="#">mls qos srr-queue input dscp-map</a>	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
	<a href="#">mls qos srr-queue input priority-queue</a>	Configures the ingress priority queue and guarantees bandwidth.
	<a href="#">mls qos srr-queue input threshold</a>	Assigns WTD threshold percentages to an ingress queue.
	<a href="#">mls qos srr-queue output cos-map</a>	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
	<a href="#">mls qos srr-queue output dsep-map</a>	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	<a href="#">policy-map</a>	Create or modifies a policy map.
	<a href="#">queue-set</a>	Maps a port to a queue-set.
	<a href="#">srr-queue bandwidth limit</a>	Limits the maximum output on a port.
	<a href="#">srr-queue bandwidth shape</a>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
	<a href="#">srr-queue bandwidth share</a>	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
<b>cos-dscp</b>	(Optional) Display class of service (CoS)-to-DSCP map.
<b>cos-input-q</b>	(Optional) Display the CoS input queue threshold map.
<b>cos-output-q</b>	(Optional) Display the CoS output queue threshold map.
<b>dscp-cos</b>	(Optional) Display DSCP-to-CoS map.
<b>dscp-input-q</b>	(Optional) Display the DSCP input queue threshold map.
<b>dscp-mutation</b> <i>dscp-mutation-name</i>	(Optional) Display the specified DSCP-to-DSCP-mutation map.
<b>dscp-output-q</b>	(Optional) Display the DSCP output queue threshold map.
<b>ip-prec-dscp</b>	(Optional) Display the IP-precedence-to-DSCP map.
<b>policed-dscp</b>	(Optional) Display the policed-DSCP map.
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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
<a href="#">mls qos map</a>	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.
<a href="#">mls qos srr-queue input cos-map</a>	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue input dscp-map</a>	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue output cos-map</a>	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue output dscp-map</a>	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

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

## Command Modes

User EXEC

## Command History

Release	Modification
12.1(11)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
	<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to the queue-set.
	<a href="#">mls qos queue-set output threshold</a>	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** | **remote**}] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

<b>session</b> <i>session_number</i>	(Optional) Specify the number of the SPAN or RSPAN session. The range is 1 to 66.
<b>all</b>	Specify all sessions.
<b>local</b>	Specify local sessions.
<b>remote</b>	Specify remote sessions.
<b>begin</b>	Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	Display excludes lines that match the <i>expression</i> .
<b>include</b>	Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

## Command Modes

User EXEC

## Command History

Release	Modification
12.1(11)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 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
  TX Only:      None
  Both:         Fa2/0/1-2, Fa4/0/1-5
Source VLANs:
  RX Only:      None
  TX Only:      None
  Both:         None
Source RSPAN VLAN:None
Destination Ports:Fa2/0/18
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** privileged EXEC command for RSPAN source session 1:

```

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

```

---

**Related Commands**

Command	Description
<a href="#">monitor session</a>	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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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
	<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
	<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
	<a href="#">show mvr interface</a>	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the <b>interface</b> and <b>members</b> keywords are appended to the command.
	<a href="#">show mvr members</a>	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

<i>interface-id</i>	(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).
<b>members</b>	(Optional) Display all MVR groups to which the specified interface belongs.
<b>vlan</b> <i>vlan-id</i>	(Optional) Display all MVR group members on this VLAN. The range is 1 to 4094.
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(11)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
<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
<a href="#">show mvr</a>	Displays the global MVR configuration on the switch.
<a href="#">show mvr members</a>	Displays all receiver ports that are members of an MVR multicast group.

# show mvr members

Use the **show mvr members** privileged EXEC command to display all receiver and source ports that are currently members of an IP multicast group.

```
show mvr members [ip-address] [ | {begin | exclude | include} expression]
```

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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
<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
<a href="#">show mvr</a>	Displays the global MVR configuration on the switch.
<a href="#">show mvr interface</a>	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the <b>members</b> 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

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

## Command Modes

User EXEC

## Command History

Release	Modification
12.1(11)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
```

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

```
Switch> show pagp 1 internal
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode.
Timers: H - Hello timer is running.      Q - Quit timer is running.
      S - Switching timer is running.    I - Interface timer is running.

Channel group 1

```

Port	Flags	State	Timers	Hello Interval	Partner Count	PAGP Priority	Learning Method	Group Ifindex
Gi1/0/1	SC	U6/S7	H	30s	1	128	Any	16
Gi1/0/2	SC	U6/S7	H	30s	1	128	Any	16

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

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

Channel group 1 neighbors

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Flags	Partner Group 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
<a href="#">clear pagp</a>	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

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



## Note

Though visible in the command-line help string, 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
	<a href="#">policy-map</a>	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] [| {begin | exclude | include} expression]
```

Syntax Description	
<b>interface</b> <i>interface-id</i>	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, stack member, module, and port number).
<b>address</b>	(Optional) Display all secure MAC addresses on all ports or a specified port.
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

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

**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.

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 : 1
Max Addresses limit in System : 1024
```

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 : 1
Max Addresses limit in System : 1024
```

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
```

#### Related Commands

Command	Description
<a href="#">switchport port-security</a>	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	
<i>vlan-ids</i>	(Optional) Display configuration information for a single VLAN identified by VLAN ID number or a range of VLANs separated by a hyphen. For <i>vlan-id</i> , the range is 1 to 4094.
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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
	<b>show running-config</b>	Displays the running configuration on the switch. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
	<b>vlan (global configuration)</b>	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).
	<b>vlan database</b>	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 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] [ | {begin | exclude | include} expression]
```

Syntax Description		
<b>default</b>	(Optional) Display the template that balances system resources among features.	
<b>routing</b>	(Optional) Display the template that maximizes system resources for routing.	
<b>vlan</b>	(Optional) Display the template that maximizes system resources for Layer 2 VLANs.	
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .	
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .	
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

**Command Modes** Privileged EXEC

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

**Usage Guidelines** If you did not reload the switch after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template currently in use and not the newly configured template.

The numbers displayed for each 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
The current template is vlan 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
```

This is an example of output from the **show sdm prefer default** command:

```
Switch# show sdm prefer default
"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 qos aces:                   512
number of security aces:              1K
```

This is an example of output from the **show sdm prefer routing** command on a switch, displaying the routing template characteristics:

```
Switch# show sdm prefer routing
"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
```

#### Related Commands

Command	Description
<a href="#">sdm prefer</a>	Sets the SDM template to maximize resources for routing or VLANs or to the default template.

# 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 | 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]
```

## Syntax Description

<i>bridge-group</i>	(Optional) Specify the bridge group number. The range is 1 to 255.
<b>active</b> [ <b>detail</b> ]	(Optional) Display spanning-tree information only on active interfaces (only available in privileged EXEC mode).
<b>backbonefast</b>	(Optional) Display spanning-tree BackboneFast status (only available in privileged EXEC mode).
<b>blockedports</b>	(Optional) Display blocked port information (only available in privileged EXEC mode).
<b>bridge</b> [ <b>address</b>   <b>detail</b>   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>priority</b> [ <b>system-id</b> ]   <b>protocol</b> ]	(Optional) Display status and configuration of this switch (only available in privileged EXEC mode).
<b>detail</b> [ <b>active</b> ]	(Optional) Display a detailed summary of interface information (only available in privileged EXEC mode).
<b>inconsistentports</b>	(Optional) Display inconsistent port information (only available in privileged EXEC mode).
<b>interface</b> <i>interface-id</i> [ <b>active</b> [ <b>detail</b> ]   <b>cost</b>   <b>detail</b> [ <b>active</b> ]   <b>inconsistency</b>   <b>portfast</b>   <b>priority</b>   <b>rootcost</b>   <b>state</b> ]	(Optional) Display spanning-tree information for the specified interface (all options only available in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels. The valid VLAN range is 1 to 4094. The valid port-channel range is 1 to 12.
<b>pathcost method</b>	(Optional) Display the default path cost method (only available in privileged EXEC mode).

<b>root</b> [ <b>address</b>   <b>cost</b>   <b>detail</b>   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>port</b>   <b>priority</b> [ <b>system-id</b> ]]	(Optional) Display root switch status and configuration (all options only available in privileged EXEC mode).
<b>summary</b> [ <b>totals</b> ]	(Optional) Display a summary of port states or the total lines of the spanning-tree state section (only available in privileged EXEC mode).
<b>uplinkfast</b>	(Optional) Display spanning-tree UplinkFast status (only available in privileged EXEC mode).
<b>vlan</b> <i>vlan-id</i> [ <b>active</b>   <b>detail</b> ]   <b>backbonefast</b>   <b>blockedports</b>   <b>bridge</b> [ <b>address</b>   <b>detail</b>   <b>forward-time</b>   <b>hello-time</b>   <b>id</b>   <b>max-age</b>   <b>priority</b> [ <b>system-id</b> ]   <b>protocol</b> ]	(Optional) Display spanning-tree information for the specified VLAN (only available in privileged EXEC mode). The range is 1 to 4094.
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes**

User EXEC; indicated keywords available only in privileged EXEC mode

**Command History**

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

**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
Bridge group 1
  Spanning tree enabled protocol vlan-bridge
  Root ID      Priority      32761
              Address      0003.fd63.2f40
              This bridge is the root
              Hello Time 10 sec  Max Age 31 sec  Forward Delay 21 sec

  Bridge ID    Priority      32761
              Address      0003.fd63.2f40
              Hello Time 10 sec  Max Age 31 sec  Forward Delay 21 sec
              Aging Time 300

Interface      Port ID      Designated      Port ID
Name           Prio.Nbr     Cost Sts        Cost Bridge ID   Prio.Nbr
-----
Vl1            128.2        6 FWD           0 32761 0003.fd63.2f40 128.2

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority      32768
              Address      0001.425b.1c40
              Cost          57
              Port          3 (GigabitEthernet1/0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID    Priority      32769 (priority 32768 sys-id-ext 1)
              Address      0003.fd63.2f00
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  305

Interface      Port ID      Designated      Port ID
Name           Prio.Nbr     Cost Sts        Cost Bridge ID   Prio.Nbr
-----
Gi1/0/1        128.3        19 FWD           38 32768 0002.b9d7.3240 128.15
Gi1/0/2        128.4        19 FWD           57 32769 0003.fd63.2f00 128.4
Gi1/0/23       128.25       19 FWD           57 32769 0003.fd63.2f00 128.25
St1            128.571      100 FWD          57 32769 0003.fd63.2f00 128.571
Gi2/0/37       128.93       200000 FWD         0 32768 0003.fd63.2f00 128.93
St2            128.572      2000000 FWD          0 32768 0003.fd63.2f00 128.572

<output truncated>
```

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

```
Switch# show spanning-tree detail

Bridge group 1 is executing the vlan-bridge compatible Spanning Tree protocol
Bridge Identifier has priority 32761, address 0003.fd63.2f40
Configured hello time 10, max age 31, forward delay 21
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 2 last change occurred 00:02:52 ago
      from Vlan1
```

```

Times: hold 1, topology change 52, notification 10
      hello 10, max age 31, forward delay 21
Timers: hello 9, topology change 0, notification 0, aging 300

```

```

Port 2 (Vlan1) of Bridge group 1 is forwarding
  Port path cost 6, Port priority 128, Port Identifier 128.2.
  Designated root has priority 32761, address 0003.fd63.2f40
  Designated bridge has priority 32761, address 0003.fd63.2f40
  Designated port id is 128.2, designated path cost 0
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  BPDU: sent 94, received 28

```

<output truncated>

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

```
Switch# show spanning-tree interface gigabitethernet1/0/1
```

Vlan Name	Port ID Prio.Nbr	Cost	Sts	Designated Cost	Bridge ID	Port ID Prio.Nbr
VLAN0001	128.3	19	FWD	38 32768	0002.b9d7.3240	128.15

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

```
Switch# show spanning-tree summary
```

```

Root bridge for: Bridge group 1, VLAN0002, VLAN0004, VLAN0006, VLAN0031,
VLAN0032, VLAN0033, VLAN0034, VLAN0035, VLAN0036, VLAN0037, VLAN0038,
VLAN0039, VLAN0040, VLAN0041, VLAN0042, VLAN0043, VLAN0044, VLAN0045,
VLAN0046, VLAN0047, VLAN0048, VLAN0049, VLAN0050, VLAN0051, VLAN0052,
VLAN0053, VLAN0054, VLAN0055, VLAN0056, VLAN0057, VLAN0058, VLAN0066,
VLAN0100, VLAN0200, VLAN0201, VLAN1000.

```

```
Extended system ID is enabled.
```

```
PortFast BPDU Guard is disabled
```

```
EtherChannel misconfiguration guard is enabled
```

```
UplinkFast is disabled
```

```
BackboneFast is disabled
```

```
Default pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
Bridge group 1	0	0	0	0	0
1 bridge	0	0	0	0	0

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

	Blocking	Listening	Learning	Forwarding	STP Active
Total	109	0	0	47	156

Related Commands	Command	Description
	<a href="#">spanning-tree backbonefast</a>	Enables the BackboneFast feature.
	<a href="#">spanning-tree bpdufilter</a>	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
	<a href="#">spanning-tree bpduguard</a>	Puts a port in the error-disabled state when it receives a BPDU.
	<a href="#">spanning-tree cost</a>	Sets the path cost for spanning-tree calculations.
	<a href="#">spanning-tree extend system-id</a>	Enables the extended system ID feature.
	<a href="#">spanning-tree guard</a>	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
	<a href="#">spanning-tree port-priority</a>	Configures an interface priority.
	<a href="#">spanning-tree portfast (global configuration)</a>	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.
	<a href="#">spanning-tree portfast (interface configuration)</a>	Enables the Port Fast feature on an interface and all its associated VLANs.
	<a href="#">spanning-tree uplinkfast</a>	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
	<a href="#">spanning-tree vlan</a>	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	
<i>interface-id</i>	(Optional) Interface ID for the physical port (including type, stack member, module, and port number).
<b>broadcast</b>	(Optional) Display broadcast storm threshold setting.
<b>multicast</b>	(Optional) Display multicast storm threshold setting.
<b>unicast</b>	(Optional) Display unicast storm threshold setting.
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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 2-18 describes the fields in the **show storm-control** display.

**Table 2-18 show storm-control Field Descriptions**

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: <ul style="list-style-type: none"> <li>Blocking—Storm control is enabled, and a storm has occurred.</li> <li>Forwarding—Storm control is enabled, and no storms have occurred.</li> <li>Inactive—Storm control is disabled.</li> </ul>
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
<b>storm-control</b>	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	
<i>stack-member-number</i>	(Optional) Display information for the specified stack member. The range is 1 to 9.
<b>detail</b>	(Optional) Display detailed information about the stack ring.
<b>neighbors</b>	(Optional) Display the neighbors for the entire switch stack.
<b>stack-ports</b>	(Optional) Display port information for the entire switch stack.
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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.

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.

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
```

Switch#	Role	Mac Address	Priority	Current State
6	Slave	0003.e31a.1e00	1	Ready

This example shows how to display summary information about a switch stack:

```
Switch(config)# show switch
```

Switch#	Role	Mac Address	Priority	Current 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
```

Switch#	Role	Mac Address	Priority	Current State
6	Slave	0003.e31a.1e00	1	Ready
*8	Master	0003.e31a.1200	1	Ready

  

Switch#	Stack Port		Neighbors	
	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
	<a href="#">reload</a>	Saves the configuration change and restarts the stack member.
	<a href="#">remote command</a>	Monitors all or specified stack members.
	<a href="#">session</a>	Accesses a specific stack member.
	<a href="#">switch priority</a>	Changes the stack member priority value.
	<a href="#">switch renumber</a>	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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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
	<a href="#">system mtu</a>	Sets the MTU size for the Fast Ethernet or Gigabit Ethernet ports.

# show uddld

Use the **show uddld** user EXEC command to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

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

Syntax Description		
<i>interface-id</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094.	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .	
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .	
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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 uddld 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 2-19](#) describes the fields in this display.

```
Switch> show uddld 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 2-19 show udd 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
	<b>uddl (global configuration)</b>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	<b>uddl (interface configuration)</b>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>uddl</b> global configuration command.
	<b>uddl reset</b>	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	
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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(0.0.145)AX, CISCO DEVELOPMENT
TEST VERSION
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 19-Feb-03 06:31 by antonino
Image text-base: 0x00003000, data-base: 0x007BFBD8

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.1(0.0.130)EA1, CISCO DEVEL
OPMENT TEST VERSION

switch uptime is 1 week, 3 hours, 42 minutes
System returned to ROM by power-on
System image file is "flash:c3750-i5-mz.121.0.0.145-AX/c3750-i5-mz.121.0.0.145-A
X.bin"

cisco WS-C3750-48-E (PowerPC405) processor with 55286K/10240K bytes of memory.
Processor board ID 123456789
Last reset from power-on
Bridging software.
9 Virtual Ethernet/IEEE 802.3 interface(s)
168 FastEthernet/IEEE 802.3 interface(s)
66 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      : 00:03:FD:63:2B:00
System serial number          : 123456789
```

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
1	52	WS-C3750-48-E	12.1(0.0.145)AX	C3750-I5-M
2	28	WS-C3750G-24TS-E	12.1(0.0.145)AX	C3750-I5-M
3	52	WS-C3750-48-E	12.1(0.0.145)AX	C3750-I5-M
*	4	WS-C3750-48-E	12.1(0.0.145)AX	C3750-I5-M
5	24	WS-C3750G-24T-E	12.1(0.0.145)AX	C3750-I5-M
6	26	WS-C3750-24-E	12.1(0.0.145)AX	C3750-I5-M

```
Switch 01
-----
```

```
Switch Uptime                : 1 day, 6 hours, 57 minutes
Base ethernet MAC Address    : 00:03:FD:63:37:00
```

```
Switch 02
-----
```

```
Switch Uptime                : 1 week, 3 hours, 43 minutes
Base ethernet MAC Address    : 00:03:FD:63:65:00
Motherboard assembly number  : 73-7058-04
Power supply part number     : 341-0045-01
Motherboard serial number    : CSJ0639002M
Power supply serial number   : PHI26004902
Model revision number        : 01
Motherboard revision number  : 04
Model number                  : WS-C3750-24TS-SMI
System serial number         : CSJ0640U01A
```

```
<output truncated>
```

# 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

<b>brief</b>	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
<b>id</b> <i>vlan-id</i>	(Optional) Display information about a single VLAN identified by VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094.
<b>internal usage</b>	(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 <b>vlan</b> global configuration command until you remove them from internal use.
<b>name</b> <i>vlan-name</i>	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
<b>remote-span</b>	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
<b>summary</b>	(Optional) Display VLAN summary information.
<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



## Note

Though visible in the command-line help string, the **ifindex** 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 2-20](#) 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
-----
```

**Table 2-20** 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.

**Table 2-20 show vlan Command Output Fields (continued)**

Field	Description
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
```

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
	<a href="#">switchport mode</a>	Configures the VLAN membership mode of a port.
	<a href="#">vlan (global configuration)</a>	Enables config-vlan mode where you can configure VLANs 1 to 4094.
	<a href="#">vlan (VLAN configuration)</a>	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	
<i>mapname</i>	(Optional) Name of a specific VLAN access map.
<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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_0_3_in_ip
  Action:
    forward
```

Related Commands	Command	Description
	<a href="#">show vlan filter</a>	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
	<a href="#">vlan access-map</a>	Creates a VLAN map entry for VLAN packet filtering.
	<a href="#">vlan filter</a>	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	Parameter	Description
	<b>access-map</b> <i>name</i>	(Optional) Display filtering information for the specified VLAN access map.
	<b>vlan</b> <i>vlan-id</i>	(Optional) Display filtering information for the specified VLAN. The range is 1 to 4094.
	<b>  begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
	<b>  exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
	<b>  include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(11)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
	<a href="#">show vlan access-map</a>	Displays information about a particular VLAN access map or all VLAN access maps.
	<a href="#">vlan access-map</a>	Creates a VLAN map entry for VLAN packet filtering.
	<a href="#">vlan filter</a>	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.
	<b>begin</b>	(Optional) Display begins with the line that matches the <i>expression</i> .
	<b>exclude</b>	(Optional) Display excludes lines that match the <i>expression</i> .
	<b>include</b>	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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 vmmps statistics** command. [Table 2-21](#) describes each field in the display.

```
Switch> show vmmps statistics
VMPS Client Statistics
-----
VQP Queries:                0
VQP Responses:              0
VMPS Changes:                0
VQP Shutdowns:              0
VQP Denied:                  0
VQP Wrong Domain:           0
VQP Wrong Version:          0
VQP Insufficient Resource:  0
```

**Table 2-21** *show vmmps 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
<b>vmmps reconfirm</b> (privileged EXEC)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.
<b>vmmps retry</b>	Configures the per-server retry count for the VQP client.
<b>vmmps server</b>	Configures the primary VMPS and up to three secondary servers.

# show vtp

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

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

Syntax Description		
<b>counters</b>		Display the VTP statistics for the switch.
<b>status</b>		Display general information about the VTP management domain status.
<b>  begin</b>		(Optional) Display begins with the line that matches the <i>expression</i> .
<b>  exclude</b>		(Optional) Display excludes lines that match the <i>expression</i> .
<b>  include</b>		(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

**Command Modes** User EXEC

Command History	Release	Modification
	12.1(11)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 vtp counters** command. [Table 2-22](#) 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 2-22 show vtp counters Field Descriptions**

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	<p>Number of revision errors.</p> <p>Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments.</p> <p>Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations.</p> <p>These errors means that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of configuration digest errors	<p>Number of MD5 digest errors.</p> <p>Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same.</p> <p>These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>

**Table 2-22 show vtp counters Field Descriptions (continued)**

Field	Description
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 2-23](#) 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 2-23 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 2-23** show vtp status Field Descriptions (continued)

Field	Description
VTP Operating Mode	<p>Displays the VTP operating mode, which can be server, client, or transparent.</p> <p>Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from nonvolatile RAM (NVRAM) after reboot. By default, every switch is a VTP server.</p> <p><b>Note</b> The switch automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning.</p> <p>Client: a switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.</p> <p>Transparent: a switch in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</p>
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
MD5 Digest	A 16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

**Related Commands**

Command	Description
<b>clear vtp counters</b>	Clears the VTP and pruning counters.
<b>vtp (global configuration)</b>	Configures the VTP filename, interface name, domain name, and mode.
<b>vtp (VLAN configuration)</b>	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
	<a href="#">show interfaces</a>	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*

<b>Syntax Description</b>	<i>vlan-id</i>	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.
---------------------------	----------------	---

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(11)AX	This command was first introduced.

<b>Usage Guidelines</b>	The <b>shutdown vlan</b> command does not change the VLAN information in the VTP database. It shuts down traffic locally, but the switch still advertises VTP information.
-------------------------	--

<b>Examples</b>	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.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>shutdown</b>	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the (config-vlan mode) <b>vlan</b> <i>vlan-id</i> global configuration command).
	<b>vlan database</b>	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** [**bridge** | **cluster** | **config** | **entity** | **envmon** | **fru-ctrl** | **hsrp** | **mac-notification** | **rtr** | **snmp** | **vlan-membership** | **vtp**]

**no snmp-server enable traps** [**bridge** | **cluster** | **config** | **entity** | **envmon** | **fru-ctrl** | **hsrp** | **mac-notification** | **rtr** | **snmp** | **vlan-membership** | **vtp**]

Syntax Description		
<b>bridge</b>	(Optional)	Generate STP bridge MIB traps.
<b>cluster</b>	(Optional)	Enable cluster traps.
<b>config</b>	(Optional)	Enable SNMP configuration traps.
<b>entity</b>	(Optional)	Enable SNMP entity traps.
<b>envmon</b>	(Optional)	Generate environmental monitor traps.
<b>fru-ctrl</b>	(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.
<b>hsrp</b>	(Optional)	Enable Hot Standby Router Protocol (HSRP) traps.
<b>mac-notification</b>	(Optional)	Enable MAC address notification traps.
<b>rtr</b>	(Optional)	Enable SNMP Response Time Reporter traps.
<b>snmp</b>	(Optional)	Enable SNMP traps.
<b>vlan-membership</b>	(Optional)	Enable SNMP VLAN membership traps.
<b>vtp</b>	(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.

### 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.

**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
<b>show running-config</b>	Displays the running configuration on the switch. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
<a href="#">snmp-server host</a>	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}] community-string [bridge | cluster
| config | entity | envmon | fru-ctrl | hsrp | mac-notification | rtr | snmp | tty | udp-port |
vlan-membership | vtp]
```

```
no snmp-server host host-addr [informs | traps] [version {1 | 2c}] community-string [bridge |
cluster | config | entity | envmon | fru-ctrl | hsrp | mac-notification | rtr | snmp | tty | udp-port |
vlan-membership | vtp]
```

### Syntax Description

<i>host-addr</i>	Name or Internet address of the host (the targeted recipient).
<b>informs</b>   <b>traps</b>	(Optional) Send SNMP traps or informs to this host.
<b>version 1</b>   <b>2c</b>	(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps.  These keywords are supported:  <b>1</b> —SNMPv1. This option is not available with informs. <b>2c</b> —SNMPv2C.  <b>Note</b> Though visible in the command-line help string, the <b>v3</b> keyword (SNMPv3) is not supported.
<i>community-string</i>	Password-like community string sent with the notification operation. Though you can set this string by using the <b>snmp-server host</b> command, we recommend that you define this string by using the <b>snmp-server community</b> global configuration command before using the <b>snmp-server host</b> command.
<b>bridge</b>	(Optional) Send SNMP Spanning Tree Protocol (STP) bridge MIB traps.
<b>cluster</b>	(Optional) Send cluster member status traps.
<b>config</b>	(Optional) Send SNMP configuration traps.
<b>entity</b>	(Optional) Send SNMP entity traps.
<b>envmon</b>	(Optional) Generate environmental monitor traps.
<b>fru-ctrl</b>	(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.
<b>hsrp</b>	(Optional) Send Hot Standby Router Protocol (HSRP) traps.
<b>mac-notification</b>	(Optional) Send MAC notification traps.
<b>rtr</b>	(Optional) Send SNMP Response Time Reporter traps.
<b>snmp</b>	(Optional) Send SNMP-type traps.
<b>tty</b>	(Optional) Send Transmission Control Protocol (TCP) connection traps.
<b>udp-port</b>	(Optional) Configure the User Datagram Protocol (UDP) port number of the host to receive the traps.
<b>vlan-membership</b>	(Optional) Send SNMP VLAN membership traps.
<b>vtp</b>	(Optional) Send VLAN Trunking Protocol (VTP) traps.

**Defaults**

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is version 1.

**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.

**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
<b>show running-config</b>	Displays the running configuration on the switch. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
<b>snmp-server enable traps</b>	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	removed
	Enable the MAC notification trap whenever a MAC address is added on this interface.	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 interface 1/0/4 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
	<b>clear mac-address-table notification</b>	Clears the MAC address notification global counters.
	<b>mac-address-table notification</b>	Enables the MAC address notification feature.
	<b>show mac-address-table notification</b>	Displays the MAC address notification settings for all interfaces or on the specified interface when the <b>interface</b> keyword is appended.
	<b>snmp-server enable traps</b>	Sends the SNMP MAC notification traps when the <b>mac-notification</b> 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** 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
	<b>show spanning-tree summary</b>	Displays a summary of the spanning-tree port states.

# spanning-tree bpdudfilter

Use the **spanning-tree bpdudfilter** 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 bpdudfilter** { **disable** | **enable** }

**no spanning-tree bpdudfilter**

Syntax Description	disable	Disable BPDU filtering on the specified interface.
	enable	Enable BPDU filtering on the specified interface.

**Defaults** BPDU filtering is disabled.

**Command Modes** Interface configuration

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

## Usage Guidelines



### Caution

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled ports by using the **spanning-tree portfast bpdudfilter default** global configuration command.

You can use the **spanning-tree bpdudfilter** interface configuration command to override the setting of the **spanning-tree portfast bpdudfilter default** global configuration command.

## Examples

This example shows how to enable the BPDU filtering feature on a port on stack member 2:

```
Switch(config)# interface fastethernet2/0/1
Switch(config-if)# spanning-tree bpdudfilter enable
```

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the current operating configuration. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
	<b>spanning-tree portfast (global configuration)</b>	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.
	<b>spanning-tree portfast (interface configuration)</b>	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

<b>disable</b>	Disable BPDU guard on the specified interface.
<b>enable</b>	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 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-if)# spanning-tree bpduguard enable
```

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the current operating configuration. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
	<b>spanning-tree portfast (global configuration)</b>	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.
	<b>spanning-tree portfast (interface configuration)</b>	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	
<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN ID associated with a spanning-tree instance. The range is 1 to 4094.
<b>cost</b>	Path cost 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: <ul style="list-style-type: none"> <li>• 1000 Mbps—4</li> <li>• 100 Mbps—19</li> <li>• 10 Mbps—100</li> </ul>

Command Modes	
	Interface configuration

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

Usage Guidelines	
	When you configure the cost, higher values represent higher costs.
	If you configure an interface with both the <b>spanning-tree vlan</b> <i>vlan-id</i> <b>cost</b> <i>cost</i> command and the <b>spanning-tree cost</b> <i>cost</i> command, the <b>spanning-tree vlan</b> <i>vlan-id</i> <b>cost</b> <i>cost</i> 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-if)# spanning-tree cost 250
```

This example shows how to set the path cost to 300 for VLAN 10:

```
Switch(config-if)# spanning-tree vlan 10 cost 300
```

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Related Commands	Command	Description
	<b>show spanning-tree interface</b> <i>interface-id</i>	Displays spanning-tree information for the specified interface.
	<b>spanning-tree port-priority</b>	Configures an interface priority.
	<b>spanning-tree vlan priority</b>	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 3750 switch supports the 802.1T spanning-tree extensions, and some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree plus [PVST+] or an instance identifier for the multiple spanning tree [MST]). In earlier releases, the switch priority is a 16-bit value.

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance. 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 vlan”](#) section.

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
<a href="#">show spanning-tree summary</a>	Displays a summary of spanning-tree port states.
<a href="#">spanning-tree vlan priority</a>	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	Command	Description
	<b>loop</b>	Enable loop guard.
	<b>none</b>	Disable root guard or loop guard.
	<b>root</b>	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

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.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports.

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-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-if)# spanning-tree guard loop
```

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

### Related Commands

Command	Description
<b>show running-config</b>	Displays the current operating configuration. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
<a href="#">spanning-tree cost</a>	Sets the path cost for spanning-tree calculations.
<a href="#">spanning-tree loopguard default</a>	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
<a href="#">spanning-tree port-priority</a>	Configures an interface priority.
<a href="#">spanning-tree vlan priority</a>	Sets the switch priority for the specified spanning-tree instance.

# 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** Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in per-VLAN spanning-tree (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.

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
	<b>show running-config</b>	Displays the current operating configuration. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
	<b>spanning-tree guard loop</b>	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 the per-VLAN spanning-tree (PVST) on your switch.

**spanning-tree mode {pvst}**

Syntax Description	
<b>pvst</b>	Enable PVST.



### Note

Though visible in the command-line help strings, the **no** version of this command is not supported.

Defaults	
	The default mode is PVST.

Command Modes	
	Global configuration

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the current operating configuration. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .

# 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	
<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN ID associated with a spanning-tree instance. The range is 1 to 4094.
<i>priority</i>	Number from 0 to 252, in increments of 4. The lower the number, the higher the priority.

**Defaults** The default is 128.

**Command Modes** Interface configuration

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

**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 Fast 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-if)# spanning-tree vlan 20 port-priority 0
```

You can verify your settings by entering the **show spanning-tree interface *interface-id*** privileged EXEC command.

Related Commands	Command	Description
	<b>show spanning-tree interface</b> <i>interface-id</i>	Displays spanning-tree information for the specified interface.
	<b>spanning-tree cost</b>	Sets the path cost for spanning-tree calculations.
	<b>spanning-tree vlan priority</b>	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 setting.

**spanning-tree portfast { bpdupfilter default | bpduguard default | default }**

**no spanning-tree portfast { bpdupfilter default | bpduguard default | default }**

Syntax Description		
<b>bpdupfilter default</b>	Globally enable BPDU filtering on Port Fast-enabled ports and prevent the switch port connected to end stations from sending or receiving BPDUs.	
<b>bpduguard default</b>	Globally enable the BPDU guard feature on Port Fast-enabled ports and place the ports that receive BPDUs in an error-disabled state.	
<b>default</b>	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

Use the **spanning-tree portfast bpdupfilter default** global configuration command to globally enable BPDU filtering on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state). The ports still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled port, the port loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdupfilter default** global configuration command by using the **spanning-tree bdpupfilter** interface configuration command.



### Caution

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bpduguard** interface configuration command.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking ports. Configure Port Fast only on ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all ports unless they are individually configured with the **spanning-tree portfast** interface configuration command.

## Examples

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking ports:

```
Switch(config)# spanning-tree portfast default
```

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

## Related Commands

Command	Description
<b>show running-config</b>	Displays the current operating configuration. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
<a href="#">spanning-tree bpdufilter</a>	Prevents a port from sending or receiving BPDUs.
<a href="#">spanning-tree bpduguard</a>	Puts a port in the error-disabled state when it receives a BPDU.
<a href="#">spanning-tree portfast (interface configuration)</a>	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.
	<b>trunk</b>	(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.

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-if)# spanning-tree portfast
```

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

**Related Commands**

Command	Description
<b>show running-config</b>	Displays the current operating configuration. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .
<a href="#">spanning-tree bpdufilter</a>	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
<a href="#">spanning-tree bpduguard</a>	Puts a port in the error-disabled state when it receives a BPDU.
<a href="#">spanning-tree portfast (global configuration)</a>	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**

**no spanning-tree uplinkfast**

## Syntax Description

This command has no arguments or keywords.



### Note

Though visible in the command-line help strings, the **max-update-rate** keyword is not supported.

## Defaults

UplinkFast is disabled.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Use this command only on access switches.

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.

---

**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**

<b>Command</b>	<b>Description</b>
<b>show spanning-tree summary</b>	Displays a summary of the spanning-tree port states.
<b>spanning-tree vlan root primary</b>	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	
<i>vlan-id</i>	VLAN ID associated with a spanning-tree instance. The range is 1 to 4094.
<b>forward-time</b> <i>seconds</i>	Set the forward-delay time for the specified spanning-tree instance. The forwarding time determines how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
<b>hello-time</b> <i>seconds</i>	Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
<b>max-age</b> <i>seconds</i>	Set the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
<b>priority</b> <i>priority</i>	Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that a standalone switch or a switch in the stack 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.
<b>root primary</b>	Force this switch to be the root switch.
<b>root secondary</b>	Set this switch to be the root switch should the primary root switch fail.
<b>diameter</b> <i>net-diameter</i>	Set the maximum number of switches between any two end stations. The range is 2 to 7.

### Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

### Command Modes

Global configuration

**Command History**

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

**Usage Guidelines**

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

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

When disabling or re-enabling the STP, you must use a single command line to specify each VLAN that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age *seconds***, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan *vlan-id* root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan *vlan-id* root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan *vlan-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

**Examples**

This example shows how to disable the STP on VLAN 5:

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

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

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

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

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 hello-time 3
```

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

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

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100:

```
Switch(config)# no spanning-tree vlan 100 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

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

#### Related Commands

Command	Description
<a href="#">show spanning-tree vlan</a>	Displays spanning-tree information.
<a href="#">spanning-tree cost</a>	Sets the path cost for spanning-tree calculations.
<a href="#">spanning-tree guard</a>	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
<a href="#">spanning-tree port-priority</a>	Sets an interface priority.
<a href="#">spanning-tree portfast (global configuration)</a>	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.
<a href="#">spanning-tree portfast (interface configuration)</a>	Enables the Port Fast feature on an interface in all its associated VLANs.
<a href="#">spanning-tree uplinkfast</a>	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) ports, but you can configure speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation.

## Syntax Description

<b>10</b>	Port runs at 10 Mbps.
<b>100</b>	Port runs at 100 Mbps.
<b>1000</b>	Port runs at 1000 Mbps. This option is valid and visible only on Gigabit Ethernet (Tx) ports.
<b>auto</b>	Port automatically detects the speed it should run at based on the port at the other end of the link.
<b>nonegotiate</b>	Autonegotiation is disabled and the port runs at 1000 Mbps. This option is valid and visible only on SFP ports.

## 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 ports, but you can configure speed to not negotiate (**nonegotiate**) if connected to a device that does not support autonegotiation.

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, configure duplex and speed on both interfaces; do use the **auto** setting on the supported side.

If both the speed and duplex are set to specific values, autonegotiation is disabled.

**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
<b>duplex</b>	Specifies the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports.
<b>show interfaces</b>	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**

<b>Syntax Description</b>	<i>weight1</i> Percentage of the port speed to which the port should be limited. The range is 10 to 90.
---------------------------	---

<b>Defaults</b>	The port is not rate limited and is set to 100 percent.
-----------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(11)AX	This command was first introduced.

<b>Usage Guidelines</b>	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.

<b>Examples</b>	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
	<b>mls qos queue-set output buffers</b>	Allocates buffers to the queue-set.
	<b>mls qos srr-queue output cos-map</b>	Maps class of service (CoS) values to egress queue or maps CoS values to a queue and to a threshold ID.
	<b>mls qos srr-queue output dscp-map</b>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	<b>mls qos queue-set output threshold</b>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue-set.
	<b>queue-set</b>	Maps a port to a queue-set.
	<b>show mls qos interface queueing</b>	Displays quality of service (QoS) information.
	<b>srr-queue bandwidth shape</b>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
	<b>srr-queue bandwidth share</b>	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
```

<b>Syntax Description</b>	<p><i>weight1 weight2 weight3 weight4</i> Specify the weights to determine the percentage of the port that is shaped. The inverse ratio (<i>1/weight</i>) determines the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.</p>				
<b>Defaults</b>	Weight1 is set to 25. Weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.				
<b>Command Modes</b>	Interface configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th data-bbox="341 976 609 1018">Release</th> <th data-bbox="625 976 1497 1018">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="341 1018 609 1060">12.1(11)AX</td> <td data-bbox="625 1018 1497 1060">This command was first introduced.</td> </tr> </tbody> </table>	Release	Modification	12.1(11)AX	This command was first introduced.
Release	Modification				
12.1(11)AX	This command was first introduced.				
<b>Usage Guidelines</b>	<p>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.</p> <p>The shaped mode overrides the shared mode.</p> <p>If you configure a shaped queue weight to 0 by using the <b>srr-queue bandwidth shape</b> interface configuration command, this queue participates in shared mode. The weight specified with the <b>srr-queue bandwidth shape</b> command is ignored, and the weights specified with the <b>srr-queue bandwidth share</b> interface configuration command for a queue come into effect.</p> <p>When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.</p>				
 <b>Note</b>	<p>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.</p>				

**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
<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to a queue-set.
<a href="#">mls qos srr-queue output cos-map</a>	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue output dscp-map</a>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
<a href="#">queue-set</a>	Maps a port to a queue-set.
<a href="#">show mls qos interface queueing</a>	Displays quality of service (QoS) information.
<a href="#">srr-queue bandwidth share</a>	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
<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to a queue-set.
<a href="#">mls qos srr-queue output cos-map</a>	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue output dscp-map</a>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
<a href="#">queue-set</a>	Maps a port to a queue-set.
<a href="#">show mls qos interface queueing</a>	Displays quality of service (QoS) information.
<a href="#">srr-queue bandwidth shape</a>	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		
	<b>broadcast</b>	Enable broadcast storm control on the interface.
	<b>multicast</b>	Enable multicast storm control on the interface.
	<b>unicast</b>	Enable unicast storm control on the interface.
	<i>level</i>	Storm-control suppression level as a percent of total bandwidth. The range is 0 to 100 percent.
	<i>.level</i>	(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
<a href="#">show storm-control</a>	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

<b>priority</b> <i>new-priority-value</i>	Specify the new stack member priority value. The range is 1 to 15.
<i>stack-member-number</i>	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
<a href="#">reload</a>	Resets the stack member and puts a configuration change into effect.
<a href="#">session</a>	Accesses a specific stack member.
<a href="#">switch renumber</a>	Changes the stack member number.
<a href="#">show switch</a>	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.
	<i>current-stack-member-number</i>		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
	<a href="#">reload</a>	Resets the stack member and puts a configuration change into effect.
	<a href="#">session</a>	Accesses a specific stack member.
	<a href="#">switch priority</a>	Changes the stack member priority value.
	<a href="#">show switch</a>	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
	<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	<b>show running-config</b>	Displays the current operating configuration. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 &gt; Cisco IOS File Management Commands &gt; Configuration File Commands</b> .

# 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

<b>vlan</b> <i>vlan-id</i>	Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094.
<b>vlan dynamic</b>	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 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
<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
<b>switchport mode</b>	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

<b>multicast</b>	Specify that unknown multicast traffic should be blocked.
<b>unicast</b>	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
<b>show interfaces switchport</b>	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 effect 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
	<a href="#">show interfaces switchport</a>	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 {auto | desirable} | trunk}
```

## Syntax Description

<b>access</b>	Set the port to access mode (either static-access or dynamic-access depending on the setting of the <b>switchport access vlan</b> 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.
<b>dynamic auto</b>	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.
<b>dynamic desirable</b>	Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
<b>trunk</b>	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
<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
<b>switchport access</b>	Configures a port as a static-access or dynamic-access port.

# 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
```

■ **switchport nonegotiate**

You can verify your setting by entering the **show interfaces *interface-id* switchport** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	<a href="#">switchport mode</a>	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, 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] | [maximum value] | [violation
{protect | restrict | shutdown}]
```

```
no switchport port-security [aging] [mac-address mac-address] | [maximum value] | [violation
{protect | restrict | shutdown}]
```

Syntax Description	
<b>aging</b>	(Optional) See the <a href="#">switchport port-security aging</a> command.
<b>mac-address</b> <i>mac-address</i>	(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.
<b>maximum</b> <i>value</i>	(Optional) Set the maximum number of secure MAC addresses for the interface. The range is 1 to 128. The default setting is 1.
<b>violation</b>	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is <b>shutdown</b> .
<b>protect</b>	(Optional) Set the security violation protect mode. When the number of secure MAC addresses reach 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.
<b>restrict</b>	(Optional) Set the security violation restrict mode. In this mode, a port security violation restricts data and causes the SecurityViolation counter to increment.
<b>shutdown</b>	(Optional) Set the security violation shutdown mode. In this mode, a port security violation causes the interface to immediately become error-disabled. When a secure port is in the error-disabled state, you can bring it out of this state by entering the <b>errdisable recovery cause psecure-violation</b> global configuration command, or you can manually re-enable it by entering the <b>shutdown</b> and <b>no shutdown</b> 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**.

## Command Modes

Interface configuration

**Command History**

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

**Usage Guidelines**

After you have set the maximum number of secure MAC addresses allowed on a port, you can add secure addresses to the address table by manually configuring them, by allowing the port to dynamically configure them, or by configuring some MAC addresses and allowing the rest to be dynamically configured.

**Note**

If the port shuts down or reboots, all dynamically learned addresses are removed.

You can delete dynamic secure MAC addresses from the address table by entering the **clear port-security dynamic** privileged EXEC command.

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.

You cannot configure static secure MAC addresses in the voice VLAN.

A secure port has the following limitations:

- A secure port cannot be a dynamic access port or a trunk 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.
- A secure port cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

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.

Although the maximum number of secured addresses per port is 128, the maximum number per system (switch stack) is 1024. Once this number is reached on configured ports, you cannot configure more than one secure address on a new port.

**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 gigabitethernet 2/0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

You can verify the settings for all secure ports or the specified port by using the **show port-security** privileged EXEC command.

This example shows how to configure a secure MAC address on Gigabit Ethernet port 12 on stack member 2.

```
Switch(config)# interface gigabitethernet 2/0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000
```

You can verify your settings by using the **show port-security address** privileged EXEC command.

**Related Commands**

Command	Description
<b>show port-security address</b>	Displays all the secure addresses configured on the switch.
<b>show port-security interface interface-id</b>	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 statically configured secure addresses on a particular port. Use the **no** form of this command to disable port security aging or to set the parameters to their default states.

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
```

```
no switchport port-security aging {static | time | type}
```

Syntax Description	Parameter	Description
	<b>static</b>	Enable aging for statically configured secure addresses on this port.
	<b>time</b> <i>time</i>	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.
	<b>type</b>	Set the aging type.
	<b>absolute</b>	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.
	<b>inactivity</b>	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
<a href="#">show port-security</a>	Displays the port security settings defined for the port.
<a href="#">switchport port-security</a>	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

<b>cos value</b>	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.
<b>trust</b>	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
	<a href="#">show interfaces</a>	Displays the administrative and operational status of a switching (nonrouting) port.
	<a href="#">switchport voice vlan</a>	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

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
	<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
	<b>switchport block</b>	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 vlan-list} | {encapsulation {dot1q | isl | negotiate}} |
  {native vlan vlan-id} | {pruning vlan vlan-list}
```

## Syntax Description

<b>allowed vlan <i>vlan-list</i></b>	Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following <i>vlan-list</i> format. The <b>none</b> keyword is not valid. The default is <b>all</b> .
<b>encapsulation dot1q</b>	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.
<b>encapsulation isl</b>	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.
<b>encapsulation negotiate</b>	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.
<b>native vlan <i>vlan-id</i></b>	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.
<b>pruning vlan <i>vlan-list</i></b>	Set the list of VLANs that are eligible for VTP pruning when in trunking mode. The <b>all</b> keyword is not valid.

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [,*vlan-atom*...]

- **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 2 to 1001; 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 2 to 1001; extended-range VLAN IDs are valid in some cases.



**Note** You cannot remove VLAN 1 or VLANs 1002 to 1005 from the list. You can remove extended-range VLANs 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 2 to 1001. 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.

### 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:

- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.
- You cannot remove VLAN 1 or VLANs 1002 to 1005 from the allowed VLAN list.

## 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
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
<a href="#">switchport mode</a>	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

<i>vlan-id</i>	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.
<b>dot1p</b>	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.
<b>none</b>	Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
<b>untagged</b>	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 **dot1p**, **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.

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
<b>show interfaces <i>interface-id</i> switchport</b>	Displays the administrative and operational status of a switching (nonrouting) port.
<b>switchport priority extend</b>	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		
<b>jumbo bytes</b>	Set the system jumbo frame size (MTU) for Gigabit Ethernet ports. The range is 1500 to 9000 bytes.	
<b>mtu bytes</b>	Set the system MTU for Fast Ethernet (10/100) . The range is 1500 to 1546 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 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 settings by entering the **show system mtu** privileged EXEC command.

---

**Related Commands**

Command	Description
<a href="#">show system mtu</a>	Displays the maximum packet size set for Fast Ethernet ports and Gigabit Ethernet ports.