

# rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics, which include usage 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*]

<b>Syntax Description</b>	<i>index</i>	Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535.
	<i>owner name</i>	(Optional) Owner of the RMON collection.

**Defaults** The RMON statistics collection is disabled.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was 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*:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# rmon collection stats 2 owner root
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show rmon statistics</b>	Displays RMON statistics.

# sdm prefer

To configure the template used in Switch Database Management (SDM) resource allocation, use the **sdm prefer** global configuration command. Use the **no** form of this command to return to the default template.

**sdm prefer** { **default** | **lanbase-routing** | **dual-ipv4-and-ipv6** { **default** | **routing** } | **qos** | **routing** }

**no sdm prefer**

## Syntax Description

<b>default</b>	Provides balance to all Layer 2 features.
<b>lanbase-routing</b>	Provides maximum system usage for configuring IPv4 static routes on SVIs.
<b>dual-ipv4-and-ipv6</b> { <b>default</b>   <b>routing</b> }	<p>Selects a template that supports both IPv4 and IPv6 routing.</p> <ul style="list-style-type: none"> <li>• <b>default</b>—Provides balance to IPv4 and IPv6 Layer 2 functionality.</li> <li>• <b>routing</b>—Provides maximum system usage for IPv4 and IPv6 routing, including IPv4 policy-based routing. You must use the IPv4 and IPv6 routing template on switches running the IP Services image for Layer 3 functionality.</li> </ul> <p>To enable IPv6 features, you must configure a dual IPv4 and IPv6 template.</p>
<b>qos</b>	Provides maximum system usage for quality of service (QoS) access control entries (ACEs).
<b>routing</b>	Provides maximum system usage for IPv4 unicast routing. You must use the routing template on switches running the IP Services image for Layer 3 functionality.

## Defaults

The **default** template provides a balance to all features.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(44)EX	This command was introduced.
12.2(52)SE	The <b>routing</b> and <b>dual-ipv4-and-ipv6 routing</b> keywords were added on switches running the IP services image.
15.0(2)SE	The <b>lanbase-routing</b> keyword was added.

## Usage Guidelines

You must reload the switch for the configuration to take effect.

If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

Use the **no sdm prefer** command to set the switch to the default template.

You must use a routing template on switches running the IP Services image for Layer 3 functionality.

Do not use the routing template if you are not using Layer 3 functionality 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.

Do not use the dual IPv4 and IPv6 template if you do not plan to enable IPv6 functionality on the switch. Entering the **sdm prefer ipv4-and-ipv6** global configuration command divides resources between IPv4 and IPv6, limiting those allocated to IPv4 forwarding.

[Table 2-1](#) shows the resources allowed for each feature in the IPv4 templates and [Table 2-2](#) shows the feature allocation in the dual IPv4 and IPv6 templates.

**Table 2-1 Approximate Number of Feature Resources Allowed by IPv4 Templates**

Resource	Default	LAN Base	QoS	Routing
Unicast MAC addresses	8 K	8 K	8 K	2 K
IGMP groups and multicast routes	256	256	256	1 K
Unicast routes	0	750		4 K
• Directly connected hosts	0	750		2 K
• Indirect routes	0	16		2 K
Policy-based routing ACEs	0	0		512
QoS classification ACEs	375	375	625	625
Security ACEs	375	375	125	375
Layer 2 VLANs	1 K	1 K	1 K	1 K

The first eight rows in the tables (unicast MAC addresses through security ACEs) represent approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance. The last row is a guideline used to calculate hardware resource consumption related to the number of Layer 2 VLANs on the switch.

**Table 2-2 Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates<sup>1</sup>**

Resource	IPv4-and-IPv6 Default	IPv4-and-IPv6 Routing
Unicast MAC addresses	8 K	1 K
IPv4 IGMP groups and multicast routes	0.25 K	0.5 K
Total IPv4 unicast routes	0	2 K
• Directly connected IPv4 hosts	0	1 K
• Indirect IPv4 routes	0	1 K
IPv6 multicast groups	0.375 K	0.625 K
Total IPv6 unicast routes	0	1.375 K
• Directly connected IPv6 addresses	0	1 K
• Indirect IPv6 unicast routes	0	0.375 K
IPv4 policy-based routing ACEs	0	0.125 K

**Table 2-2** *Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates<sup>1</sup> (continued)*

Resource	IPv4-and-IPv6 Default	IPv4-and-IPv6 Routing
IPv4 or MAC QoS ACEs (total)	0.375 K	0.375 K
IPv4 or MAC security ACEs (total)	0.375 K	0.125 K
IPv6 policy-based routing ACEs <sup>2</sup>	0	0.125 K
IPv6 QoS ACEs	0	0.125 K
IPv6 security ACEs	0.125 K	0.125 K

1. Template estimates are based on a switch with 8 routed interfaces and approximately 1000 VLANs.

2. IPv6 policy-based routing is not supported.

## Examples

This example shows how to use the QoS template:

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

This example shows how to configure the dual IPv4 and IPv6 default template on a switch:

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
```

This example shows how to configure the IPv4 and IPv6 routing template on a switch:

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 routing
Switch(config)# exit
Switch# reload
Proceed with reload? [confirm]
```

## 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 to enable the password-recovery mechanism (the default). This mechanism allows an end user with physical access to the switch to hold down the **Express Setup** button and interrupt the bootup 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 bootup process is allowed only if the user agrees to set the system back to the default configuration.

**service password-recovery**

**no service password-recovery**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	The password-recovery mechanism is enabled.
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	As a system administrator, you can use the <b>no service password-recovery</b> 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, you must have physical access to the switch.

To delete the switch password and set a new one, follow these steps:

- |               |   |
|---------------|---|
| <b>Step 1</b> | Press the <b>Express Setup</b> button until the SETUP LED blinks green and the LED of an available switch downlink port blinks green.<br><br>If no switch downlink port is available for your PC or laptop connection, disconnect a device from one of the switch downlink ports. Press the <b>Express Setup</b> button again until the SETUP LED and the port LED blink green. |
| <b>Step 2</b> | Connect your PC or laptop to the port with the blinking green LED.<br><br>The SETUP LED and the switch downlink port LED stop blinking and stay solid green.  |
| <b>Step 3</b> | Press and hold the <b>Express Setup</b> button. Notice that the SETUP LED starts blinking green again. Continue holding the button until the SETUP LED turns solid green (approximately 5 seconds). Release the <b>Express Setup</b> button immediately.  |

This procedure deletes the password without affecting any other configuration settings. You can now access the switch without a password through the console port or by using the device manager.

- Step 4** Enter a new password through the device manager by using the Express Setup window or through the command line interface by using the **enable secret** global configuration command.

**Note**

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

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

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

**Examples**

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

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

**Related Commands**

Command	Description
<a href="#">show version</a>	Displays version information for the hardware and firmware.

# service-policy

Use the **service-policy** interface configuration command to apply a policy map defined by the **policy-map** command to the input of a physical port or a switch virtual interface (SVI). Use the **no** form of this command to remove the policy map and port 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 a physical port or an SVI.



### Note

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

## Defaults

No policy maps are attached to the port.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(44)EX	This command was introduced.
12.2(52)SE	A policy map can now be applied to a physical port or an SVI.

## Usage Guidelines

Only one policy map per ingress port is supported.

Policy maps can be configured on physical ports or on SVIs. When VLAN-based quality of service (QoS) is disabled by using the **no mls qos vlan-based** interface configuration command on a physical port, you can configure a port-based policy map on the port. If VLAN-based QoS is enabled by using the **mls qos vlan-based** interface configuration command on a physical port, the switch removes the previously configured port-based policy map. After a hierarchical policy map is configured and applied on an SVI, the interface-level policy map takes effect on the interface.

You can apply a policy map to incoming traffic on a physical port or on an SVI. You can configure different interface-level policy maps for each class defined in the VLAN-level policy map. For more information about hierarchical policy maps, see the “Configuring QoS” chapter in the software configuration guide for this release.

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 physical ingress port:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input plcmap1
```

This example shows how to remove *plcmap2* from a physical port:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no service-policy input plcmap2
```

This example shows how to apply *plcmap1* to an ingress SVI when VLAN-based QoS is enabled:

```
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input plcmap1
```

This example shows how to create a hierarchical policy map and attach it to an SVI:

```
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
.
.
.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input gigabitethernet1/1 - gigabitethernet1/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class-map cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class-map cm-1
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class-map cm-2
Switch(config-pmap-c)# match ip dscp 2
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class-map cm-3
Switch(config-pmap-c)# match ip dscp 3
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap-c)# exit
Switch(config-pmap)# class-map cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# exit
Switch(config)# interface vlan 10
Switch(config-if)#
Switch(config-if)# ser input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
```

## Related Commands

Command	Description
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.



Command	Description
<a href="#">show policy-map</a>	Displays QoS policy maps.
show running-config	Displays the running configuration on the switch. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 &gt; File Management Commands &gt; Configuration File Management Commands</b> .

# set

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

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

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

## Syntax Description

<b>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</b> ] <b>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.

## Defaults

No traffic classification is defined.

## Command Modes

Policy-map class configuration

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

If you have used the **set ip dscp** policy-map class configuration command, the switch changes this command to **set dscp** in the switch configuration. If you enter the **set ip dscp** policy-map class configuration command, this setting appears as **set dscp** in the switch configuration.

You can use the **set ip precedence** policy-map class configuration command or the **set precedence** policy-map class configuration command. This setting appears as **set ip precedence** in the switch configuration.

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

For the **set 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 dscp af11** command, which is the same as entering the **set 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 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 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 ports to specify a service policy.
<b>show policy-map</b>	Displays 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
	12.2(44)EX	This command was 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 NVRAM or return to the setup program or the command-line prompt without saving it.

**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
GigabitEthernet1/1	unassigned	YES	unset	up	up
GigabitEthernet1/2	unassigned	YES	unset	up	down

<output truncated>

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 GigabitEthernet1/1
no ip address
!
interface GigabitEthernet1/2
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, Release 12.2 &gt; File Management Commands &gt; Configuration File Management Commands</b> .
<b>show version</b>	Displays version information for the hardware and firmware.

# setup express

Use the **setup express** global configuration command to enable Express Setup mode. Use the **no** form of this command to disable Express Setup mode.

**setup express**

**no setup express**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	Express Setup is enabled.
-----------------	---------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

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

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

**Note**

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

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

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

<b>Examples</b>	This example shows how to enable Express Setup mode:
-----------------	--

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

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

- On an unconfigured switch, the LEDs below the Express Setup button turn solid green after 3 seconds.
- On a configured switch, the mode LEDs begin blinking after 2 seconds and turn solid green after 10 seconds.



#### Caution

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

This example shows how to disable Express Setup mode:

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

You can verify that Express Setup mode is disabled by pressing the Express Setup button. The LEDs do not turn solid green *or* begin blinking green if Express Setup mode is not enabled on the switch.

#### Related Commands

Command	Description
<a href="#">show setup express</a>	Displays if Express Setup mode is active.



# show access-lists

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

**show access-lists** [*name* | *number* | **hardware counters** | **ipc**]

## 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>ipc</b>	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EX	This command was 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.

This command also displays the MAC ACLs that are configured.



### Note

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

**Examples**

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

```
Switch# show access-lists
Standard IP access list 1
  10 permit 1.1.1.1
  20 permit 2.2.2.2
  30 permit any
  40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
  10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
  10 permit 10.10.10.10
Extended IP access list 121
  10 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
  10 deny ip any host 19.19.11.11
  20 deny ip any host 10.11.12.13
  Dynamic Cluster-NAT permit ip any any
  10 permit ip host 10.99.100.128 any
  20 permit ip host 10.46.22.128 any
  30 permit ip host 10.45.101.64 any
  40 permit ip host 10.45.20.64 any
  50 permit ip host 10.213.43.128 any
  60 permit ip host 10.91.28.64 any
  70 permit ip host 10.99.75.128 any
  80 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 Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 &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 Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 &gt; IP Services Commands</b> .
<b>mac access-list extended</b>	Configures a named or numbered MAC access list on the switch.

# show alarm description port

Use the **show alarm description port** EXEC command to display the alarm numbers with the text description.

**show alarm description port**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Examples** This is an example of output from the **show alarm description port** command. It shows the alarmIDs and their respective alarm descriptions.

```
Switch> show alarm description port
 1      Link Fault
 2      Port Not Forwarding
 3      Port Not Operating
 4      FCS Error Rate exceeds threshold
```

Related Commands	Command	Description
	<a href="#">alarm profile (global configuration)</a>	Creates an alarm profile containing one or more alarm IDs and alarm options.
	<a href="#">show alarm profile</a>	Displays all alarm profiles or a specified alarm profile and lists the interfaces to which each profile is attached.

# show alarm profile

Use the **show alarm profile** EXEC command to display all alarm profiles configured in the system or the specified profile and the interfaces to which each profile is attached.

**show alarm profile** [*name*]

Syntax Description	<i>name</i>	(Optional) Display only the profile with the specified name.
--------------------	-------------	--

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Usage Guidelines** If you do not enter a profile name, the display includes the profile information for all existing alarm profiles. This command does not display the default configuration settings.

The *defaultPort* profile is applied by default to all interfaces. This profile enables only the Port Not Operating (3) alarm. You can use the **alarm profile defaultPort** global configuration command and modify this profile to enable other alarms.

**Examples** These are examples of output from the **show alarm profile** command.

This output displays all ports that are attached to the configured profiles.

```
Switch> show alarm profile GigE-UplinkPorts
Interface      Gi1/2
Alarms         1,2,3,4
Syslog         1,2,3,4
Notifies       1,2,3,4
Relay-major    4
Relay-minor    1,2
```

This output displays all the configured profiles:

```
Switch> show alarm profile
Alarm Profile my_gig_port:
Interface      Gi1/2
Alarms         1,2,3,4
Syslog         1,2,3,4
Notifies       1,2,3,4
Relay-major    4
Relay-minor    1,2
Alarm Profile my_fast_port:
Interface      Fa1/1
Alarms         1,2,3,4
Syslog         1,2,3,4
Notifies       1,2,3,4
Relay-major    4
Relay-minor    1,2
```

 show alarm profile

Related Commands	Command	Description
	<a href="#">alarm profile (global configuration)</a>	Creates an alarm profile containing one or more alarm IDs and alarm options.
	<a href="#">alarm profile (interface configuration)</a>	Attaches an alarm profile to an interface.

# show alarm settings

Use the **show alarm settings** EXEC command to display all environmental alarm settings on the switch.

## show alarm settings

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Examples** This is an example of output from the **show alarm settings** command. It shows all the switch alarm settings that are on the switch:

```
Switch> show alarm settings
Alarm relay mode: Positive
```

```
Power Supply
  Alarm           Enabled
  Relay           MAJ
  Notifies        Enabled
  Syslog          Enabled
Temperature-Primary
  Alarm           Enabled
  Thresholds      MAX: 95C           MIN: -20C
  Relay           MAJ
  Notifies        Enabled
  Syslog          Enabled
Temperature-Secondary
  Alarm           Disabled
  Threshold
  Relay
  Notifies        Disabled
  Syslog          Disabled
```

Related Commands	Command	Description
	<a href="#">alarm facility power-supply</a>	Sets power supply alarm options.
	<a href="#">alarm facility temperature</a>	Sets temperature alarm options.
	<a href="#">power-supply dual</a>	Sets dual power-supply mode.

# show archive status

Use the **show archive status** privileged EXEC command to display the status of a new image being downloaded to a switch with the HTTP or the TFTP protocol.

**show archive status**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Usage Guidelines** If you use the **archive download-sw** privileged EXEC command to download an image to a TFTP server, the output of the **archive download-sw** command shows the status of the download.

If you do not have a TFTP server, you can use Network Assistant or the embedded device manager to download the image by using HTTP. The **show archive status** command shows the progress of the download.

**Examples** These are examples of output from the **show archive status** command:

```
Switch# show archive status
IDLE: No upgrade in progress
```

```
Switch# show archive status
LOADING: Upgrade in progress
```

```
Switch# show archive status
EXTRACT: Extracting the image
```

```
Switch# show archive status
VERIFY: Verifying software
```

```
Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

Related Commands	Command	Description
	<a href="#">archive download-sw</a>	Downloads a new image from a TFTP server to the switch.



# show arp access-list

Use the **show arp access-list** EXEC command to display detailed information about Address Resolution Protocol (ARP) access control (lists).

**show arp access-list** [*acl-name*]

Syntax Description	<i>acl-name</i> (Optional) Name of the ACL.
--------------------	---

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Examples** This is an example of output from the **show arp access-list** command:

```
Switch> show arp access-list
ARP access list rose
  permit ip 10.101.1.1 0.0.0.255 mac any
  permit ip 20.3.1.0 0.0.0.255 mac any
```

Related Commands	Command	Description
	<a href="#">arp access-list</a>	Defines an ARP ACL.
	<a href="#">deny (ARP access-list configuration)</a>	Denies an ARP packet based on matches against the Dynamic Host Configuration Protocol (DHCP) bindings.
	<a href="#">ip arp inspection filter vlan</a>	Permits ARP requests and responses from a host configured with a static IP address.
	<a href="#">permit (ARP access-list configuration)</a>	Permits an ARP packet based on matches against the DHCP bindings.

# show authentication

Use the **show authentication** command EXEC mode to display information about authentication manager events on the switch.

**show authentication** {**interface** *interface-id* | **registrations** | **sessions** [**session-id** *session-id*] [**handle** *handle*] [**interface** *interface-id*] [**mac** *mac*] [**method** *method*] | **statistics** [**summary**]}

## Syntax Description

<b>interface</b> <i>interface-id</i>	(Optional) Display all of the authentication manager details for the specified interface.
<b>method</b> <i>method</i>	(Optional) Displays all clients authorized by a specified authentication method ( <b>dot1x</b> , <b>mab</b> , or <b>webauth</b> )
<b>registrations</b>	(Optional) Display authentication manager registrations
<b>sessions</b>	(Optional) Display detail of the current authentication manager sessions (for example, client devices). If you do not enter any optional specifiers, all current active sessions are displayed. You can enter the specifiers singly or in combination to display a specific session (or group of sessions).
<b>session-id</b> <i>session-id</i>	(Optional) Specify an authentication manager session.
<b>handle</b> <i>handle</i>	(Optional) Specify a range from 1 to 4294967295.
<b>mac</b> <i>mac</i>	(Optional) Display authentication manager information for a specified MAC address.
<b>statistics</b>	(Optional) Display authentication statistics in detail.
<b>summary</b>	(Optional) Display authentication statistics summary.

## Command Default

This command has no default settings.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

[Table 2-3](#) describes the significant fields shown in the output of the **show authentication** command.



### Note

The possible values for the status of sessions are shown below. For a session in terminal state, *Authz Success* or *Authz Failed* is displayed along with *No methods* if no method has provided a result.

**Table 2-3** *show authentication Command Output*

Field	Description
Idle	The session has been initialized and no methods have run yet.
Running	A method is running for this session.
No methods	No method has provided a result for this session.
Authc Success	A method has resulted in authentication success for this session.
Authc Failed	A method has resulted in authentication fail for this session.
Authz Success	All features have been successfully applied for this session.
Authz Failed	A feature has failed to be applied for this session.

**Table 2-4** lists the possible values for the state of methods. For a session in a terminal state, *Authc Success*, *Authc Failed*, or *Failed over* are displayed. *Failed over* means that an authentication method ran and then failed over to the next method, which did not provide a result. *Not run* appears for sessions that synchronized on standby.

**Table 2-4** *State Method Values*

Method State	State Level	Description
Not run	Terminal	The method has not run for this session.
Running	Intermediate	The method is running for this session.
Failed over	Terminal	The method has failed and the next method is expected to provide a result.
Authc Success	Terminal	The method has provided a successful authentication result for the session.
Authc Failed	Terminal	The method has provided a failed authentication result for the session.

## Examples

This is an example the **show authentication registrations** command:

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
Handle Priority Name
3 0 dot1x
2 1 mab
1 2 webauth
```

This is an example of the **show authentication interface interface-id** command:

```
Switch# show authentication interface gigabitEthernet1/2
Client list:
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/2
Available methods list:
Handle Priority Name
3 0 dot1x
Runnable methods list:
Handle Priority Name
3 0 dot1x
```

This is an example of the **show authentication sessions** command:

```
Switch# show authentication sessions
Interface  MAC Address      Method  Domain  Status      Session ID
Gi3/45     (unknown)          N/A     DATA   Authz Failed 0908140400000007003651EC
Gi3/46     (unknown)          N/A     DATA   Authz Success 09081404000000080057C274
```

This is an example of the **show authentication sessions** command for a specified interface:

```
Switch# show authentication sessions int gigabitethernet 1/4
Interface: GigabitEthernet0/46 GigabitEthernet1/4
MAC Address: Unknown
IP Address: Unknown
Status: Authz Success
Domain: DATA
Oper host mode: multi-host
Oper control dir: both
Authorized By: Guest Vlan
Vlan Policy: 4094
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 09081404000000080057C274
Acct Session ID: 0x0000000A
Handle: 0xCC000008
Runnable methods list:
Method  State
dot1x   Failed over
```

This is an example of the **show authentication sessions** command for a specified MAC address:

```
Switch# show authentication sessions mac 000e.84af.59bd
Interface: GigabitEthernet1/4
MAC Address: 000e.84af.59bd
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0xE0000000
Runnable methods list:
Method State
dot1x Authc Success
```

This is an example of the **show authentication session method** command for a specified method:

```
Switch# show authentication sessions method mab
No Auth Manager contexts match supplied criteria
Switch# show authentication sessions method dot1x
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/23
```

## Related Commands

Command	Description
<a href="#">authentication control-direction</a>	Configures the port mode as unidirectional or bidirectional.
<a href="#">authentication event</a>	Sets the action for specific authentication events.
<a href="#">authentication fallback</a>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<a href="#">authentication host-mode</a>	Sets the authorization manager mode on a port.

Command	Description
<b>authentication open</b>	Enables or disables open access on a port.
<b>authentication order</b>	Sets the order of authentication methods used on a port.
<b>authentication periodic</b>	Enables or disables reauthentication on a port.
<b>authentication port-control</b>	Enables manual control of the port authorization state.
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.

# show auto qos

Use the **show auto qos** EXEC command to display the quality of service (QoS) commands entered on the interfaces on which automatic QoS (auto-QoS) is enabled.

**show auto qos** [**interface** *interface-id*]

## Syntax Description

<b>interface</b> <i>interface-id</i>	(Optional) Display auto-QoS information for the specified port or for all ports. Valid interfaces include physical ports.
--------------------------------------	---

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

The **show auto qos** command output shows only the auto-QoS command entered on each interface. The **show auto qos interface** *interface-id* command output shows the auto-QoS command entered on a specific interface.

Use the **show running-config** privileged EXEC command to display the auto-QoS configuration and the user modifications.

The **show auto qos** command output also shows the service policy information for the Cisco IP phone.

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

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

## Examples

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

```
Switch> show auto qos
```

```
GigabitEthernet1/1
auto qos voip cisco-softphone
```

```
GigabitEthernet1/3
auto qos voip cisco-phone
```

```
GigabitEthernet1/2
auto qos voip cisco-phone
```

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

```
Switch> show auto qos interface gigabitethernet 1/1
```

```
GigabitEthernet1/1
auto qos voip cisco-phone
```

This is an example of output from the **show running-config** privileged EXEC command when the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Switch# show running-config
Building configuration...
...
mls qos map policed-dscp 24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 75 75 75 250
mls qos queue-set output 1 threshold 3 75 150 100 300
mls qos queue-set output 1 threshold 4 50 100 75 400
mls qos queue-set output 2 threshold 1 100 100 100 100
mls qos queue-set output 2 threshold 2 35 35 35 35
mls qos queue-set output 2 threshold 3 55 82 100 182
mls qos queue-set output 2 threshold 4 90 250 100 400
mls qos queue-set output 1 buffers 15 20 20 45
mls qos queue-set output 2 buffers 24 20 26 30
```

```

mls qos
...
!
class-map match-all AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp cs3 af31
!
policy-map AutoQoS-Police-SoftPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
!
policy-map AutoQoS-Police-CiscoPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
...
!
interface FastEthernet1/1
  switchport mode access
  switchport port-security maximum 1999
  speed 100
  duplex full
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  auto qos voip cisco-phone
!

interface GigabitEthernet1/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 2
  switchport mode access
  speed 10
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  auto qos voip cisco-phone
!

interface GigabitEthernet1/2
  srr-queue bandwidth share 10 10 60 20
  priority-queue out
  mls qos trust device cisco-phone
  mls qos trust cos
  mls qos trust device cisco-phone
  service-policy input AutoQoS-Police-CiscoPhone

```

<output truncated>

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

```
Switch> show auto qos interface FastEthernet1/2
```

```
FastEthernet1/2
```



```
auto qos voip cisco-softphone
```

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

```
Switch> show auto qos
AutoQoS not enabled on any interface
```

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

```
Switch> show auto qos interface gigabitethernet1/1
AutoQoS is disabled
```

#### Related Commands

Command	Description
<a href="#">auto qos voip</a>	Automatically configures QoS for VoIP within a QoS domain.
<a href="#">debug auto qos</a>	Enables debugging of the auto-QoS feature.

# show boot

To display the settings of the boot environment variables, use the **show boot** command in privileged EXEC mode.

## show boot

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Examples</b>	This is an example of output from the <b>show boot</b> command. <a href="#">Table 2-5</a> describes each field in the display.
-----------------	--

```
Switch# show boot
```

```
Switch# show boot
BOOT path-list : flash:/ie2k-universalk9-mz.150-0.27.SE/ie3000-universalk9-mz
.150-0.27.EY.bin
Config file : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break : yes
Manual Boot : no
HELPER path-list :
Auto upgrade : yes
Auto upgrade path :
Boot optimization : disabled
NVRAM/Config file
buffer size: 65536
Timeout for Config
Download: 0 seconds
Config Download
via DHCP: disabled (next boot: disabled)
Switch#
```

**Table 2-5** *show boot Field Descriptions*

Field	Description
BOOT path-list	Displays a semicolon separated list of executable files to try to load and execute when automatically booting up.  If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.  If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot up with the first bootable file that it can find in the flash file system.
Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Enable Break	Displays whether a break during booting up is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic bootup 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 up. If it is set to no or 0, the bootloader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the bootloader mode.
Helper path-list	Displays a semicolon separated list of loadable files to dynamically load during the bootloader initialization. Helper files extend or patch the functionality of the bootloader.
Auto upgrade	Displays whether the switch is set to automatically copy its software version to an incompatible switch.
Boot optimization	Displays whether the switch is set to minimize the time to boot up after a system failure.
NVRAM/Config file buffer size	Displays the buffer size that Cisco 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 Cisco 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 up the switch during the next bootup cycle.
	<b>boot private-config-file</b>	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration.
	<b>boot system</b>	Specifies the Cisco IOS image to load during the next bootup cycle.
	<b>boot fast</b>	Enables fast booting during the next bootup cycle.

# show cable-diagnostics tdr

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

**show cable-diagnostics tdr interface** *interface-id*

<b>Syntax Description</b>	<i>interface-id</i> Specify the interface on which TDR was run.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	For more information about TDR, see the software configuration guide for this release.
-------------------------	--

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

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

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

```
Switch# show cable-diagnostics tdr interface fa0/1
```

```
TDR test last run on: March 01 01:05:40
```

Interface	Speed	Local pair	Pair length	Remote pair	Pair status
Fa0/1	100M	Pair A	N/A	Pair A	Normal
		Pair B	N/A	Pair A	Normal
		Pair C	N/A	Pair A	N/A
		Pair D	N/A	Pair A	N/A

Table 2-6 lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

**Table 2-6** Fields Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	Interface on which TDR was run.
Speed	Speed of connection.
Local pair	Name of the pair of wires that TDR is testing on the local interface.
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases: <ul style="list-style-type: none"> <li>The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s.</li> <li>The cable is open.</li> <li>The cable has a short.</li> </ul>
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: <ul style="list-style-type: none"> <li>Normal—The pair of wires is properly connected.</li> <li>Not completed—The test is running and is not completed.</li> <li>Not supported—The interface does not support TDR.</li> <li>Open—The pair of wires is open.</li> <li>Shorted—The pair of wires is shorted.</li> <li>ImpedanceMis—The impedance is mismatched.</li> <li>Short/Impedance Mismatched—The impedance mismatched or the cable is short.</li> <li>InProgress—The diagnostic test is in progress</li> </ul>

This is an example of output from the **show interfaces** *interface-id* command when TDR is running:

```
Switch# show interfaces gigabitethernet1/2
```

```
gigabitethernet1/2 is up, line protocol is up (connected: TDR in Progress)
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/2
```

```
% TDR test was never issued on Gi1/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on switch 1
```

**Related Commands**

Command	Description
<a href="#">test cable-diagnostics tdr</a>	Enables and runs TDR on an interface.

# show cip

Use the **show cip** privileged EXEC command to display information about the Common Industrial Protocol (CIP) subsystem.

**show cip {connection | faults | file | miscellaneous | object | security | session | status}**

## Syntax Description

<b>connection</b>	Display the CIP connection information.
<b>faults</b>	Display information about CIP faults.
<b>file</b>	Display the information about the CIP file instances.
<b>miscellaneous</b>	Display miscellaneous CIP system information.
<b>object</b>	Display information about specific CIP objects. These objects include assembly, Ethernet link, identity, switch parameter, time sync, and TCP/IP objects.
<b>security</b>	Display the CIP security window status and settings.
<b>session</b>	Display the active and inactive CIP sessions.
<b>status</b>	Display the CIP status (enabled or disabled).

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.
12.2(50)SE	The <b>faults</b> keyword was added.

## Examples

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

```
Switch# show cip faults
Major/Minor Recoverable Faults
-----
MAC address flap :          Normal
CDP native vlan mismatch : Normal
Storm control event :       Normal
Port security violation :    Normal
Port in error-disable state: Normal
Major Unrecoverable Faults
-----
POST detected HW failure : Normal
SFP in error-disable state : Normal
```

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

```
Switch# show cip security
State : Enabled
Password: abc123
Window: Open
Owner IP: 172.20.140.147
Window timeout: 600 seconds
Window open tick: 17
```

 show cip

Related Commands	Command	Description
	<a href="#">cip enable</a>	Enables CIP on a VLAN.
	<a href="#">cip security</a>	Sets CIP security options on the switch.



# show cisp

Use the **show cisp** privileged EXEC command to display CISP information for a specified interface.

**show cisp** {[*interface interface-id*] | **clients** | **summary**}

Syntax Description	<b>clients</b>	(Optional) Display CISP client details
	<b>interface</b> <i>interface-id</i>	(Optional) Display CISP information about the specified interface. Valid interfaces include physical ports and port channels.
	<b>summary</b>	(Optional) Display

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

Command History	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

## Examples

This example shows output from the **show cisp interface** command:

```
WS-C3750E-48TD#show cisp interface fast 0
CISP not enabled on specified interface
```

This example shows output from the **show cisp summary** command:

```
CISP is not running on any interface
```

Related Commands	<b>Command</b>	<b>Description</b>
	<b>dot1x credentials</b> <i>profile</i>	Configure a profile on a supplicant switch
	<b>cisp enable</b>	Enable Client Information Signalling Protocol (CISP)

# show class-map

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

**show class-map** [*class-map-name*]

<b>Syntax Description</b>	<i>class-map-name</i> (Optional) Display the contents of the specified class map.
---------------------------	---

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Examples</b>	<p>This is an example of output from the <b>show class-map</b> command:</p> <pre>Switch&gt; 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</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<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** 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

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	If you enter this command on a switch that is not a cluster member, the error message <code>Not a management cluster member</code> appears.
-------------------------	---

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, 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.
--

<b>Examples</b>	This is an example of output when the <b>show cluster</b> command is entered on the active cluster command switch:
-----------------	--

<pre>Switch&gt; show cluster Command switch for cluster "cluster1 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:                 cluster1_standby     Standby Group Number:         110 Heartbeat interval:               8 Heartbeat hold-time:              80 Extended discovery hop count:     3</pre>
--

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 "cluster2"
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
<b>cluster enable</b>	Enables a command-capable switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it.
<b>show cluster candidates</b>	Displays a list of candidate switches.
<b>show cluster members</b>	Displays information about the cluster members.

# show cluster candidates

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

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

<b>Syntax Description</b>	<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>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	This command is available only on the 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 <i>switch member number</i> . 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 <i>switch member number</i> is the upstream neighbor of the candidate switch. The hop count is the number of devices the candidate is from the cluster command switch.

<b>Examples</b>	This is an example of output from the <b>show cluster candidates</b> command:
-----------------	---

```
Switch> show cluster candidates
00d0.7961.c4c0 StLouis-2    WS-IE3000-4TC   Gi1/1          2    1   Fa1/1
00d0.bbf5.e900 ldf-dist-128 WS-C3524-XL    Fa1/7          1    0   Fa0/24
00e0.1e7e.be80 1900_Switch  1900           3          0    1    0   Fa0/11
00e0.1e9f.7a00 Surfers-24    WS-C2924-XL    Fa1/5          1    0   Fa0/3
00e0.1e9f.8c00 Surfers-12-2  WS-C2912-XL    Fa1/4          1    0   Fa0/7
00e0.1e9f.8c40 Surfers-12-1  WS-C2912-XL    Fa1/1          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-IE3000-4TC
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 0)
  Local port:          Gi1/1   FEC number:
  Upstream port:       Gi2/2   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 to display information about the cluster members.

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

<b>Syntax Description</b>	<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.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

**Usage Guidelines** This command is available only on the cluster command switch.  
If the cluster has no members, this command displays an empty line at the prompt.

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

```
Switch# show cluster members

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

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

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
  Device type:          cisco WS-IE3000
  MAC address:          0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:           Gi1/1   FEC number:
  Upstream port:        Gi2/3   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-ies
  MAC address:          0002.4b29.2e00
  Upstream MAC address:
  Local port:           FEC number:
  Upstream port:        FEC Number:
```

## show cluster members

```

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-ies
  MAC address:      0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:       Gi0/1    FEC number:
  Upstream port:    Fa0/11   FEC Number:
  Hops from command device: 2
Device '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 ASIC and the send and receive statistics for packets reaching the CPU.

## show controllers cpu-interface

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

**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 19CDD00 paktail 19D02C8

<output truncated>

Supervisor ASIC Mic Registers
-----
```

**show controllers cpu-interface**

```

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 ASIC.

**show controllers ethernet-controller** [*interface-id*] [**phy** [**detail**]] [**port-asic** {**configuration** | **statistics**}] [**fastethernet 0**]

<b>Syntax Description</b>	<i>interface-id</i>	The physical interface (including type, 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. This display includes the operational state of the automatic medium-dependent interface crossover (auto-MDIX) feature on an 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>Command Modes</b>	Privileged EXEC (only supported with the <i>interface-id</i> keywords in EXEC mode)
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was 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.

**Examples**

This is an example of output from the **show controllers ethernet-controller** command for an interface. [Table 2-7](#) describes the *Transmit* fields, and [Table 2-8](#) describes the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitethernet1/1
Transmit GigabitEthernet1/1
  0 Bytes
  0 Unicast frames
  0 Multicast frames
  0 Broadcast frames
  0 Too old frames
  0 Deferred frames
  0 MTU exceeded frames
  0 1 collision frames
  0 2 collision frames
  0 3 collision frames
  0 4 collision frames
  0 5 collision frames
  0 6 collision frames
  0 7 collision frames
  0 8 collision frames
  0 9 collision frames
  0 10 collision frames
  0 11 collision frames
  0 12 collision frames
  0 13 collision frames
  0 14 collision frames
  0 15 collision frames
  0 Excessive collisions
  0 Late collisions
  0 VLAN discard frames
  0 Excess defer 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
Receive
  0 Bytes
  0 Unicast frames
  0 Multicast frames
  0 Broadcast frames
  0 Unicast bytes
  0 Multicast bytes
  0 Broadcast bytes
  0 Alignment errors
  0 FCS errors
  0 Oversize frames
  0 Undersize frames
  0 Collision fragments
  0 Minimum size frames
  0 65 to 127 byte frames
  0 128 to 255 byte frames
  0 256 to 511 byte frames
  0 512 to 1023 byte frames
  0 1024 to 1518 byte frames
  0 Overrun frames
  0 Pause frames
  0 Symbol error frames
  0 Invalid frames, too large
  0 Valid frames, too large
  0 Invalid frames, too small
  0 Valid frames, too small
  0 Too old frames
  0 Valid oversize frames
  0 System FCS error frames
  0 RxPortFifoFull drop frame
```

**Table 2-7** *Transmit Field Descriptions*

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

**Table 2-7** *Transmit Field Descriptions (continued)*

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

1. CFI = Canonical Format Indicator

**Table 2-8** *Receive Field Descriptions*

Field	Description
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS <sup>1</sup> value and the incorrectly formed frames. This value excludes the frame header bits.
Unicast frames	The total number of frames successfully received on the interface that are directed to unicast addresses.
Multicast frames	The total number of frames successfully received on the interface that are directed to multicast addresses.
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.

**Table 2-8**      **Receive Field Descriptions (continued)**

Field	Description
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast bytes	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Alignment errors	The total number of frames received on an interface that have alignment errors.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
Oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size.
Undersize frames	The number of frames received on an interface that are smaller than 64 bytes.
Collision fragments	The number of collision fragments received on an interface.
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
Overrun frames	The total number of overrun frames received on an interface.
Pause frames	The number of pause frames received on an interface.
Symbol error frames	The number of frames received on an interface that have symbol errors.
Invalid frames, too large	The number of frames received that were larger than maximum allowed MTU <sup>2</sup> size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too large	The number of frames received on an interface that are larger than the maximum allowed frame size.
Invalid frames, too small	The number of frames received that are smaller than 64 bytes (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too small	The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and that have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.
Too old frames	The number of frames dropped on the ingress port because the packet aged out.
Valid oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag.

**Table 2-8**      **Receive Field Descriptions (continued)**

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

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

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

```
Switch# show controllers ethernet-controller gigabitethernet1/1 phy
GigabitEthernet1/1 (gpn: 1, port-number: 1)
```

-----

General SFP Information

-----

```
Identifier       : 0x03
Connector       : 0x00
Transceiver     : 0x00 0x00 0x00 0x08 0x00 0x00 0x00 0x00
Encoding        : 0x01
BR_Nominal      : 0x0D
Vendor Name     : CISCO-METHODE
Vendor Part Number : SP7041
Vendor Revision  : 0x43 0x20 0x20 0x20
Vendor Serial Number : 00000MTC1017075F
-----
```

Other Information

-----

```
Port asic num    : 0
Port asic port num : 0
XCVR init completed : 0
Embedded PHY     : not present

SFP presence index : 0
SFP iter cnt      : 30
SFP failed oper flag : 0x0
IIC error cnt     : 0
IIC error dsb cnt : 0
IIC max sts cnt   : 50
Chk for link status : 1
Link Status       : 1
Link Status Media  : 2
```

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 1, PortASIC 0 Registers
```

```
-----
DeviceType       : 000101BC
Reset            : 00000000
PmadMicConfig    : 00000001
PmadMicDiag      : 00000003
SupervisorReceiveFifoSramInfo : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo : 000001D0 000001D0 40000000
```

# show controllers ethernet-controller

```

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

```

<output truncated>

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

```

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

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

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

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

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

```



```

0 Learning Cam Skip Count

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

<output truncated>
```

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 team</a>	Displays the state of registers for all ternary content addressable memory (TCAM) in the system and for TCAM interface ASICs that are CAM controllers.

# 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 ASICs that are CAM controllers.

**show controllers tcam** [**asic** **[number]**] [**detail**]

<b>Syntax Description</b>	<b>asic</b>	(Optional) Display port ASIC TCAM information.
	<b>number</b>	(Optional) Display information for the specified port ASIC number. The range is from 0 to 15.
	<b>detail</b>	(Optional) Display detailed TCAM register information.

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.
-------------------------	--

**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 controllers utilization

Use the **show controllers utilization** EXEC command to display bandwidth utilization on the switch or specific ports.

**show controllers** [*interface-id*] **utilization**

<b>Syntax Description</b>	<i>interface-id</i> (Optional) ID of the switch interface.
---------------------------	--

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

## Examples

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

```
Switch> show controllers utilization
Port      Receive Utilization  Transmit Utilization
Fa1/1      0                      0
Fa1/2      0                      0
Fa1/3      0                      0
Fa1/4      0                      0
Fa1/5      0                      0
Fa1/6      0                      0
Fa1/7      0                      0
<output truncated>
```

<output truncated>

```
Switch Receive Bandwidth Percentage Utilization : 0
Switch Transmit Bandwidth Percentage Utilization : 0
```

```
Switch Fabric Percentage Utilization : 0
```

This is an example of output from the **show controllers utilization** command on a specific port:

```
Switch> show controllers gigabitethernet1/1 utilization
Receive Bandwidth Percentage Utilization : 0
Transmit Bandwidth Percentage Utilization : 0
```

**Table 2-9** *show controllers utilization* Field Descriptions

Field	Description
Receive Bandwidth Percentage Utilization	Displays the received bandwidth usage of the switch, which is the sum of the received traffic on all the ports divided by the switch receive capacity.

**Table 2-9** *show controllers utilization Field Descriptions*

Field	Description
Transmit Bandwidth Percentage Utilization	Displays the transmitted bandwidth usage of the switch, which is the sum of the transmitted traffic on all the ports divided it by the switch transmit capacity.
Fabric Percentage Utilization	Displays the average of the transmitted and received bandwidth usage of the switch.

**Related Commands**

Command	Description
<a href="#">show controllers ethernet-controller</a>	Displays the interface internal registers.

# show dot1q-tunnel

To display information about IEEE 802.1Q tunnel ports, use the **show dot1q-tunnel** command in EXEC mode.

**show dot1q-tunnel** [**interface** *interface-id*]

Syntax Description	<b>interface</b> <i>interface-id</i>	(Optional) Specifies the interface for which to display IEEE 802.1Q tunneling information. Valid interfaces include physical ports and port channels.
--------------------	--------------------------------------	---

Command Modes	EXEC (>)
---------------	----------

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

Usage Guidelines	This command is available only when the switch is running the IP Services image.
------------------	--

**Examples** These are examples of output from the **show dot1q-tunnel** command:

```
Switch> show dot1q-tunnel
dot1q-tunnel mode LAN Port(s)
-----
Gi1/1
Gi1/2
Gi1/3
Gi1/6
Po2
```

```
Switch> show dot1q-tunnel interface gigabitethernet0/1
dot1q-tunnel mode LAN Port(s)
-----
Gi1/1
```

Related Commands	Command	Description
	<b>show vlan dot1q tag native</b>	Displays IEEE 802.1Q native VLAN tagging status.
	<b>switchport mode dot1q-tunnel</b>	Configures an interface as an IEEE 802.1Q tunnel port.

# show dot1x

Use the **show dot1x** EXEC command to display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

**show dot1x** [{**all** [**summary**] | **interface** *interface-id*} [**details** | **statistics**]]

## Syntax Description

<b>all</b> [ <b>summary</b> ]	(Optional) Display the IEEE 802.1x status for all ports.
<b>interface</b> <i>interface-id</i>	(Optional) Display the IEEE 802.1x status for the specified port (including type, module, and port number).
<b>details</b>	(Optional) Display the IEEE 802.1x interface details.
<b>statistics</b>	(Optional) Display IEEE 802.1x statistics for the specified port.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

If the port control is configured as unidirectional or bidirectional control and this setting conflicts with the switch configuration, the **show dot1x** {**all** | **interface** *interface-id*} privileged EXEC command output has this information:

ControlDirection = In (Inactive)

**Examples**

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

```
Switch> show dot1x
Sysauthcontrol           Enabled
Dot1x Protocol Version   2
Critical Recovery Delay   100
Critical EAPOL            Disabled
```

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

```
Switch> show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   2
Critical Recovery Delay   100
Critical EAPOL            Disabled

Dot1x Info for GigabitEthernet1/1
-----
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
Violation Mode            = PROTECT
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

<output truncated>
```

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

Interface	PAE	Client	Status
-----	-----	-----	-----
Gil/1	AUTH	none	UNAUTHORIZED
Gil/2	AUTH	00a0.c9b8.0072	AUTHORIZED
Fal/1 AUTH	none		UNAUTHORIZED

This is an example of output from the **show dot1x interface interface-id EXEC** command:

```
Switch> show dot1x interface gigabitethernet1/2
Dot1x Info for GigabitEthernet1/2
-----
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = In
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
```



This is an example of output from the **show dot1x interface *interface-id* details** EXEC command:

```
Switch# show dot1x interface gigabitEthernet1/2 details
Dot1x Info for GigabitEthernet1/2
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

Dot1x Authenticator Client List Empty
```

This is an example of output from the **show dot1x interface *interface-id* details** command when a port is assigned to a guest VLAN and the host mode changes to multiple-hosts mode:

```
Switch# show dot1x interface gigabitEthernet1/1 details
Dot1x Info for GigabitEthernet1/1
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Enabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0
Guest-Vlan = 182

Dot1x Authenticator Client List Empty

Port Status = AUTHORIZED
Authorized By = Guest-Vlan
Operational HostMode = MULTI_HOST
Vlan Policy = 182
```

This is an example of output from the **show dot1x interface *interface-id* statistics** command. [Table 2-10](#) describes the fields in the display.

```
Switch> show dot1x interface gigabitEthernet1/2 statistics
Dot1x Authenticator Port Statistics for GigabitEthernet1/2
-----
RxStart = 0      RxLogoff = 0      RxResp = 1      RxRespID = 1
RxInvalid = 0    RxLenErr = 0      RxTotal = 2

TxReq = 2        TxReqID = 132     TxTotal = 134

RxVersion = 2    LastRxSrcMAC = 00a0.c9b8.0072
```

**Table 2-10** *show dot1x statistics Field Descriptions*

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

**Related Commands**

Command	Description
<a href="#">dot1x default</a>	Resets the IEEE 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*]

<b>Syntax Description</b>	<b>interface</b> (Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, module, and port number).
---------------------------	--

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

## 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 gigabitethernet1/1
DTP information for GigabitEthernet1/1:
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
0 output errors
0 trunk timeouts
1 link ups, last link up on Mon Mar 01 1993, 01:02:29
0 link downs
```

 show dtp

Related Commands	Command	Description
	<a href="#">show interfaces trunk</a>	Displays interface trunking information.

# show eap

Use the **show eap** privileged EXEC command to display Extensible Authentication Protocol (EAP) registration and session information for the switch or for the specified port.

```
show eap {{registrations [method name] | transport name}} | {{sessions [credentials name
[interface interface-id] | interface interface-id | method name | transport name}} }
[credentials name | interface interface-id | transport name]
```

Syntax Description	
<b>registrations</b>	Display EAP registration information.
<b>method</b> <i>name</i>	(Optional) Display EAP method registration information.
<b>transport</b> <i>name</i>	(Optional) Display EAP transport registration information.
<b>sessions</b>	Display EAP session information.
<b>credentials</b> <i>name</i>	(Optional) Display EAP method registration information.
<b>interface</b> <i>interface-id</i>	(Optional) Display the EAP information for the specified port (including type, module, and port number).

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

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Usage Guidelines** When you use the **show eap registrations** privileged EXEC command with these keywords, the command output shows this information:

- None—All the lower levels used by EAP and the registered EAP methods.
- **method** *name* keyword—The specified method registrations.
- **transport** *name* keyword—The specific lower-level registrations.

When you use the **show eap sessions** privileged EXEC command with these keywords, the command output shows this information:

- None—All active EAP sessions.
- **credentials** *name* keyword—The specified credentials profile.
- **interface** *interface-id* keyword—The parameters for the specified interface.
- **method** *name* keyword—The specified EAP method.
- **transport** *name* keyword—The specified lower layer.

**Examples** This is an example of output from the **show eap registrations** privileged EXEC command:

```
Switch> show eap registrations
Registered EAP Methods:
  Method  Type                Name
```

## show eap

```
4      Peer      MD5
```

Registered EAP Lower Layers:

Handle	Type	Name
2	Authenticator	Dot1x-Authenticator
1	Authenticator	MAB

This is an example of output from the **show eap registrations transport** privileged EXEC command:

```
Switch> show eap registrations transport all
```

Registered EAP Lower Layers:

Handle	Type	Name
2	Authenticator	Dot1x-Authenticator
1	Authenticator	MAB

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

```
Switch> show eap sessions
```

Role:	Authenticator	Decision:	Fail
Lower layer:	Dot1x-Authentic	Interface:	Gi1/1
Current method:	None	Method state:	Uninitialised
Retransmission count:	0 (max: 2)	Timer:	Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)			
EAP handle:	0x5200000A	Credentials profile:	None
Lower layer context ID:	0x93000004	Eap profile name:	None
Method context ID:	0x00000000	Peer Identity:	None
Start timeout (s):	1	Retransmit timeout (s):	30 (30)
Current ID:	2	Available local methods:	None

Role:	Authenticator	Decision:	Fail
Lower layer:	Dot1x-Authentic	Interface:	Gi1/2
Current method:	None	Method state:	Uninitialised
Retransmission count:	0 (max: 2)	Timer:	Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)			
EAP handle:	0xA800000B	Credentials profile:	None
Lower layer context ID:	0x0D000005	Eap profile name:	None
Method context ID:	0x00000000	Peer Identity:	None
Start timeout (s):	1	Retransmit timeout (s):	30 (30)
Current ID:	2	Available local methods:	None

<Output truncated>

This is an example of output from the **show eap sessions interface interface-id** privileged EXEC command:

```
Switch# show eap sessions gigabitethernet1/1
```

Role:	Authenticator	Decision:	Fail
Lower layer:	Dot1x-Authentic	Interface:	Gi1/1
Current method:	None	Method state:	Uninitialised
Retransmission count:	1 (max: 2)	Timer:	Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)			
EAP handle:	0x5200000A	Credentials profile:	None
Lower layer context ID:	0x93000004	Eap profile name:	None
Method context ID:	0x00000000	Peer Identity:	None
Start timeout (s):	1	Retransmit timeout (s):	30 (30)
Current ID:	2	Available local methods:	None

## Related Commands

Command	Description
<b>clear eap sessions</b>	Clears EAP session information for the switch or for the specified port.

# show env

Use the **show env** EXEC command to show switch environment information.

**show env {all | power | temperature [status]}**

Syntax Description	<b>all</b>	Display both fan and temperature environmental status.
	<b>power</b>	Display the switch power status.
	<b>temperature</b>	Display the switch temperature status.
	<b>status</b>	(Optional) Display the switch internal temperature.

Command Modes	EXEC
---------------	------

Command History	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

Usage Guidelines	The command output shows the green and yellow states as <i>OK</i> and the red state as <i>FAULTY</i> .
	If you enter the <b>show env all</b> command on this switch, the command output is the same as the <b>show env temperature status</b> command output.
	For more information about the threshold levels, see the software configuration guide for this release.

Examples	This is an example of output from the <b>show env all</b> command:
----------	--

```
Switch> show env all
TEMPERATURE is OK
Temperature Value: 48 Degree Celsius
POWER SUPPLY A is DC OK
POWER SUPPLY B is DC OK
```

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

```
Switch> show env power
Power supply A is DC OK
Power supply B is DC FAULTY
```

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

```
Switch> show env temperature
Temperature is OK
```

This is an example of output from the **show env temperature status** command.

```
Switch> show env temperature status
Temperature Value: 48 Degree Celsius
```

# show errdisable detect

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

**show errdisable detect**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

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

```
Switch> show errdisable detect
ErrDisable Reason    Detection    Mode
-----
arp-inspection       Enabled     port
bpduguard            Enabled     vlan
channel-misconfig    Enabled     port
community-limit      Enabled     port
dhcp-rate-limit      Enabled     port
dtp-flap             Enabled     port
gbic-invalid          Enabled     port
inline-power          Enabled     port
invalid-policy        Enabled     port
l2ptguard            Enabled     port
link-flap            Enabled     port
loopback             Enabled     port
lsgroup              Enabled     port
pagp-flap            Enabled     port
psecure-violation    Enabled     port/vlan
security-violatio    Enabled     port
sfp-config-mismat    Enabled     port
storm-control        Enabled     port
udld                 Enabled     port
vmps                 Enabled     port
```

Related Commands	Command	Description
	<a href="#">errdisable detect cause</a>	Enables error-disabled 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-disabled 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** EXEC command to display conditions that cause an error to be recognized for a cause.

## show errdisable flap-values

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was 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

**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-disabled detection for a specific cause or all causes.
	<a href="#">show errdisable detect</a>	Displays error-disabled detection status.
	<a href="#">show errdisable recovery</a>	Displays error-disabled 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** EXEC command to display the error-disabled recovery timer information.

## show errdisable recovery

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

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

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----
udld                  Disabled
bpduguard             Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                  Disabled
pagp-flap             Disabled
dtp-flap              Disabled
link-flap             Enabled
l2ptguard             Disabled
psecure-violation    Disabled
gbic-invalid          Disabled
dhcp-rate-limit       Disabled
unicast-flood         Disabled
storm-control         Disabled
arp-inspection        Disabled
loopback              Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
-----
Gi1/2        link-flap             279
```



### Note

Though visible in the output, the unicast-flood field is not valid.

**Related Commands**

Command	Description
<a href="#">errdisable recovery</a>	Configures the recover mechanism variables.
<a href="#">show errdisable detect</a>	Displays error-disabled 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** EXEC command to display EtherChannel information for a channel.

**show etherchannel** [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}]  
{**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 6.
<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>protocol</b>	Display the protocol that is being used in the EtherChannel.
<b>summary</b>	Display a one-line summary per channel-group.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was 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 port, 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).

## Examples

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

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2    Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP

          Ports in the group:
          -----

Port: Gi1/1
-----

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

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

```

Local information:

Port      Flags   State   LACP port  Admin   Oper   Port   Port
Gi1/1     SA      bndl    32768      0x0     0x1    0x0     0x3D

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

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

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

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

Ports in the Port-channel:

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

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

```

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

```

Switch> show etherchannel 1 summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       u - unsuitable for bundling
       U - in use        f - failed to allocate aggregator
       d - default port

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

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

```

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

```

Switch> show etherchannel 1 port-channel
      Port-channels in the group:
      -----

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

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

Ports in the Port-channel:

Index   Load   Port      EC state      No of bits

```

**show etherchannel**

```

-----+-----+-----+-----+-----
0      00      Gi1/1      Active      0
0      00      Gi1/2      Active      0

```

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

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

```

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

Group: 2
-----
Protocol: PAgP

```

**Related Commands**

Command	Description
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group.
<a href="#">channel-protocol</a>	Restricts the protocol used on a port to manage channeling.
<a href="#">interface port-channel</a>	Accesses or creates the port channel.

# show facility-alarm relay

Use the **show facility-alarm relay** EXEC command to display facility alarms associated with the indicated relay circuitry.

**show facility-alarm relay {major | minor}**

Syntax Description	major	Display alarms associated with major relay.
	minor	Display alarms associated with minor relay.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Examples** This is an example of output from the **show facility-alarm relay major** command. It displays alarm information for the major relays.

```
Switch# show facility-alarm relay major
```

Source	Severity	Description	Relay	Time
Switch	MAJOR	1 Temp above max primary thresh	MAJ	Oct 06

```
Switch#
```

```
Switch> show facility-alarm relay minor
```

Source	Description	Relay	Time
Switch	1 Temp above secondary thresh	MIN	Mar 01 1993 00:0 1:17

Related Commands	Command	Description
	<a href="#">alarm facility power-supply</a>	Sets power supply alarm options.
	<a href="#">alarm facility temperature</a>	Sets temperature alarm options.
	<a href="#">alarm profile (global configuration)</a>	Creates alarm profiles with alarm IDs and alarm options to be attached to interfaces.
	<a href="#">show facility-alarm status</a>	Display alarms generated on the switch.

# show facility-alarm status

Use the **show facility-alarm status** EXEC command to display all generated alarms for the switch.

**show facility-alarm status** [**critical** | **info** | **major** | **minor**]

<b>Syntax Description</b>	<b>critical</b>	(Optional) Display only critical facility alarms.
	<b>info</b>	(Optional) Display all facility alarms.
	<b>major</b>	(Optional) Display major facility alarms and higher.
	<b>minor</b>	(Optional) Display major facility alarms and higher.

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

**Examples** This is an example of output from the **show facility-alarm status** command. It displays alarm information for the switch.

Switch# **show facility-alarm status**

```
Source          Severity Description                      Relay    Time
toyota_S16_sps1 MAJOR    1 Temp above max primary thresh MAJ      Oct 06
               Syslog                      Disabled
```

Switch> **show facility-alarm status**

```
Source          Severity Description                      Relay    Time
FastEthernet1/3 MINOR    2 Port Not Forwarding          NONE     Mar 01
1993 00:02:22
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">alarm facility power-supply</a>	Sets power supply alarm options.
	<a href="#">alarm facility temperature</a>	Sets temperature alarm options.
	<a href="#">alarm profile (global configuration)</a>	Creates alarm profiles with alarm IDs and alarm options to be attached to interfaces.
	<a href="#">show facility-alarm relay</a>	Displays alarm relays generated on the switch.



# show fallback profile

Use the **show fallback profile** privileged EXEC command to display the fallback profiles that are configured on a switch.

## show fallback profile

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Usage Guidelines** Use the **show fallback profile** privileged EXEC command to display profiles that are configured on the switch.

**Examples** This is an example of output from the **show fallback profile** command:

```
switch# show fallback profile
Profile Name: dot1x-www
-----
Description      : NONE
IP Admission Rule : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
-----
Description      : NONE
IP Admission Rule : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
-----
Description      : NONE
IP Admission Rule : NONE
IP Access-Group IN: NONE
```

Related Commands	Command	Description
	<a href="#">dot1x fallback profile</a>	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<a href="#">fallback profile profile</a>	Create a web authentication fallback profile.
	<a href="#">ip admission rule</a>	Enable web authentication on a switch port
	<a href="#">ip admission name proxy http</a>	Enable web authentication globally on a switch
	<a href="#">show dot1x [interface interface-id]</a>	Displays IEEE 802.1x status for the specified port.

# show fcs-threshold

Use the **show fcs-threshold** EXEC command to display the frame check sequence (FCS) bit error-rate settings on the switch interfaces.

## show fcs-threshold

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Usage Guidelines** The Ethernet standard calls for a maximum bit error rate of  $10^{-8}$ . In the Cisco IE 3000 switch, the configurable bit error-rate range is from  $10^{-6}$  to  $10^{-11}$ . The bit error-rate input to the switch is a positive exponent. The output displays the positive exponent; an output of 9 means that the bit error-rate is  $10^{-9}$ .

**Examples** This is an example of output from the **show fcs-threshold** command. It shows the output when all ports are set to the default FCS threshold.

```
Switch# show fcs-threshold
Port      FCS Threshold
Fa1/1      8
Fa1/2      8
Fa1/3      8
Fa1/4      8
Fa2/1      8
Fa2/2      8
Fa2/3      8
Fa2/4      8
Fa2/5      8
Fa2/6      8
Fa2/7      8
Fa2/8      8
Fa3/1      8
Fa3/2      8
Fa3/3      8
Fa3/4      8
Fa3/5      8
Fa3/6      8
Fa3/7      8
Fa3/8      8
Gi1/1      8
Gi1/2      8
```

## Related Commands

Command	Description
<a href="#">fcs-threshold</a>	Sets the FCS threshold on an interface.

# show flowcontrol

Use the **show flowcontrol** EXEC command to display the flow control status and statistics.

**show flowcontrol** [**interface** *interface-id* | **module** *number*]

<b>Syntax Description</b>	<b>interface</b> <i>interface-id</i>	(Optional) Display the flow control status and statistics for a specific interface.
	<b>module</b> <i>number</i>	(Optional) Display the flow control status and statistics for all interfaces on the switch. Module number is 1. This option is not available if you have entered a specific interface ID.

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	Use this command to display the flow control status and statistics on the switch or for a specific interface.
	Use the <b>show flowcontrol</b> command to display information about all the switch interfaces. The output from the <b>show flowcontrol</b> command is the same as the output from the <b>show flowcontrol module number</b> command.
	Use the <b>show flowcontrol interface</b> <i>interface-id</i> command to display information about a specific interface.

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

```
Switch> show flowcontrol
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
              admin    oper              admin    oper
-----
Gi1/1         Unsupp.  Unsupp.  off      off      0        0
Gi1/2         desired  off      off      off      0        0
Gi1/3         desired  off      off      off      0        0
<output truncated>
```

This is an example of output from the **show flowcontrol interface** *interface-id* command:

```
Switch> show flowcontrol gigabitethernet1/2
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
              admin    oper              admin    oper
-----
Gi1/2         desired  off      off      off      0        0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">flowcontrol</a>	Sets the receive flow-control state for an interface.

# show interfaces

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

**show interfaces** [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [*module number*] | **counters** | **description** | **etherchannel** | **flowcontrol** | **private-vlan mapping** | **rep** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** [**backup** | *module number*] | **transceiver** | **properties** | **detail** [*module number*] | **trunk**]

Syntax	Description
<i>interface-id</i>	(Optional) Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 6.
<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>Note</b> The display shows only packets processed in software; hardware-switched packets do not appear.
<b>capabilities</b>	(Optional) Display the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
<i>module number</i>	(Optional) Display <b>capabilities</b> , <b>switchport</b> configuration, or <b>transceiver</b> characteristics (depending on preceding keyword) of all interfaces on the switch. The only valid module number is 1. This option is not available if you enter a specific interface ID.
<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>private-vlan mapping</b>	(Optional) Display private-VLAN mapping information for the VLAN switch virtual interfaces (SVIs). This keyword is available only if your switch is running the IP services image, formerly known as the enhanced multilayer image (EMI).
<b>pruning</b>	(Optional) Display interface trunk VTP pruning information.
<b>rep</b>	(Optional) See the <a href="#">show interfaces rep</a> command.
<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. A status of <i>unsupported</i> in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
<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>backup</b>	(Optional) Display Flex Link backup interface configuration and status for the specified interface or all interfaces on the switch.

<b>transceiver [detail   properties]</b>	(Optional) Display the physical properties of a CWDM or DWDM small form-factor (SFP) module interface. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>detail</b>—(Optional) Display calibration properties, including high and low numbers and any alarm information.</li> <li><b>properties</b>—(Optional) Display speed and duplex settings on an interface.</li> </ul>
<b>trunk</b>	Display interface trunk information. If you do not specify an interface, only information for active trunking ports appears.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.2(44)EX	This command was introduced.
12.2(50)SE	The <b>rep</b> keyword was added.
12.2(52)SE	The <b>private-vlan mapping</b> keywords were added.

**Usage Guidelines**

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

- Use the **show interfaces capabilities module 1** to display the capabilities of all interfaces on the switch. Entering any other number is invalid.
- Use the **show interfaces *interface-id* capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces on the switch.
- Use the **show interfaces switchport module 1** to display the switch port characteristics of all interfaces on the switch. Entering any other number is invalid.

**Note**

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

**Examples**

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

```
Switch# show interface GigabitEthernet1/2
GigabitEthernet1/2 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 001e.1300.4882 (bia 001e.1300.4882)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 100Mb/s, link type is auto, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:00, 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 2000 bits/sec, 4 packets/sec
5 minute output rate 17000 bits/sec, 27 packets/sec
  553226 packets input, 39772509 bytes, 0 no buffer
    Received 530934 broadcasts (529980 multicasts)
      0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 529980 multicast, 0 pause input
    0 input packets with dribble condition detected
  4031941 packets output, 317450903 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 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.

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

<output truncated>

```

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

```

Switch# show interfaces GigabitEthernet1/2 capabilities
GigabitEthernet1/2
Model:                IE-3000-4TC
Type:                 Not Present
Speed:                10,100,1000,auto
Duplex:                half,full,auto
Trunk encap. type:    802.1Q
Trunk mode:           on,off,desirable,nonegotiate
Channel:              yes
Broadcast suppression: percentage(0-100)
Flowcontrol:          rx-(off,on,desired),tx-(none)
Fast Start:           yes
QoS scheduling:       rx-(not configurable on per port basis),
                     tx-(4q3t) (3t: Two configurable values and one fixed.)
CoS rewrite:          yes
ToS rewrite:          yes
UDLD:                 yes
Inline power:         no
SPAN:                 source/destination
PortSecure:           yes
Dot1x:                yes

```

```
Multiple Media Types: rj45, sfp, auto-select
```

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

```
Switch# show interfaces gigabitethernet1/2 description
Interface Status      Protocol Description
Gi1/2      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 interface-id pruning** command when pruning is enabled in the VTP domain:

```
Switch# show interfaces gigabitethernet1/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/2     3,4

Port      Vlans traffic requested of neighbor
Gi1/2     1-3
```

This is an example of output from the **show interfaces stats** command for a specified VLAN 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
Fa1/1     Fa1/1              notconnect  1         auto    auto  10/100BaseTX
Fa1/2     Fa1/2              notconnect  1         auto    auto  10/100BaseTX
Fa1/3     Fa1/3              notconnect  1         auto    auto  10/100BaseTX
Fa1/4     Fa1/4              notconnect  1         auto    auto  10/100BaseTX
Fa2/1     Fa2/1              notconnect  1         auto    auto  10/100BaseTX
Fa2/2     Fa2/2              notconnect  1         auto    auto  10/100BaseTX
Fa2/3     Fa2/3              notconnect  1         auto    auto  10/100BaseTX
Fa2/4     Fa2/4              notconnect  1         auto    auto  10/100BaseTX
```



```

Fa2/5                notconnect 1          auto    auto 10/100BaseTX
Fa2/6                notconnect 1          auto    auto 10/100BaseTX
Fa2/7                notconnect 1          auto    auto 10/100BaseTX
Fa2/8                notconnect 1          auto    auto 10/100BaseTX

```

<output truncated>

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 2 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25.

```

Switch# show interfaces fastethernet1/2 status
Port      Name      Status      Vlan      Duplex  Speed  Type
Fa01/2    connected 20,25      a-full    a-100   10/100BaseTX

```

In this example, port 3 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20.

```

Switch# show interfaces fastethernet1/3 status
Port      Name      Status      Vlan      Duplex  Speed  Type
Fa01/3    connected 20          a-full    a-100   10/100BaseTX

```

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
Gi1/2     err-disabled dtp-flap

```

This is an example of output from the **show interfaces switchport** command for a port. [Table 2-11](#) describes the fields in the display.



#### Note

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

```

Switch# show interfaces gigabitethernet1/1 switchport
Name: Gi1/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association:10 (VLAN0010) 502 (VLAN0502)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

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

```

Voice VLAN: none (Inactive)  
Appliance trust: none

**Table 2-11** *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.
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.
Administrative private-vlan host-association	Displays the administrative VLAN association for private-VLAN host ports.
Administrative private-vlan mapping	Displays the administrative VLAN mapping for private-VLAN promiscuous ports.
Operational private-vlan	Displays the operational private-VLAN status.
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

This is an example of output from the **show interfaces switchport** command for a port configured as a private VLAN promiscuous port. The primary VLAN 20 is mapped to secondary VLANs 25, 30, and 35:

```
Switch# show interfaces gigabitethernet1/2 switchport
Name: Gi1/2
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

```

Administrative private-vlan host-association: none
Administrative private-vlan mapping: 20 (VLAN0020) 25 (VLAN0025) 30 (VLAN0030) 35
(VLAN0035)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)
30 (VLAN0030)
35 (VLAN0035)

```

<output truncated>

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

```
Switch# show interfaces switchport backup
```

```
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
Fal/1	Fal/2	Active Up/Backup Standby
Fal/3	Fal/5	Active Down/Backup Up
Po1	Po2	Active Standby/Backup Up

This is an example of output from the **show interfaces switchport backup** command. In this example, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)#interface gigabitEthernet 1/1
```

```
Switch(config-if)#switchport backup interface gigabitEthernet 1/2 prefer vlan 60,100-120
```

When both interfaces are up, Gi1/2 forwards traffic for VLANs 60, 100 to 120, and Gi1/1 forwards traffic for VLANs 1 to 50.

```
Switch#show interfaces switchport backup
```

```
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet1/1	GigabitEthernet1/2	Active Down/Backup Up

```
Vlans on Interface Gi 1/1: 1-50
```

```
Vlans on Interface Gi 1/2: 60, 100-120
```

When a Flex Link interface goes down (LINK\_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi1/1 goes down, Gi1/2 carries all VLANs of the Flex Link pair.

```
Switch#show interfaces switchport backup
```

```
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet1/1	GigabitEthernet1/2	Active Down/Backup Up

```
Vlans on Interface Gi 1/1:
```

```
Vlans on Interface Gi 1/2: 1-50, 60, 100-120
```

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi1/1 comes up, then VLANs preferred on this interface are blocked on the peer interface Gi1/2 and forwarded on Gi1/1.

```
Switch#show interfaces switchport backup
```

Switch Backup Interface Pairs:

```

Active Interface      Backup Interface      State
-----
GigabitEthernet1/1  GigabitEthernet1/1  Active Down/Backup Up

Vlans on Interface Gi 1/1: 1-50
Vlans on Interface Gi 1/2: 60, 100-120

```

This is an example of output from the **show interfaces interface-id pruning** command:

```

Switch# show interfaces gigabitethernet1/2 pruning
Port      Vlans pruned for lack of request by neighbor

```

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

```

Switch# show interfaces gigabitethernet1/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi1/1     auto      negotiate      trunking    1

Port      Vlans allowed on trunk
Gi1/1     1-4094

Port      Vlans allowed and active in management domain
Gi1/1     1-4

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/1     1-4

```

This is an example of output from the **show interfaces interface-id transceiver properties** command:

```

Switch# show interfaces gigabitethernet1/2 transceiver properties
Name : Gi1/2
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off

```

This is an example of output from the **show interfaces interface-id transceiver detail** command:

```

Switch# show interfaces gigabitethernet1/3 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.

```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/3	41.5	110.0	103.0	-8.0	-12.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/3	3.20	4.00	3.70	3.00	2.95

	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold

Port	(milliamperes)	(mA)	(mA)	(mA)	(mA)
-----	-----	-----	-----	-----	-----
Gi1/3	31.0	84.0	70.0	4.0	2.0
	Optical	High Alarm	High Warn	Low Warn	Low Alarm
	Transmit Power	Threshold	Threshold	Threshold	Threshold
Port	(dBm)	(dBm)	(dBm)	(dBm)	(dBm)
-----	-----	-----	-----	-----	-----
Gi1/3	-0.0 ( -0.0)	-0.0	-0.0	-0.0	-0.0
	Optical	High Alarm	High Warn	Low Warn	Low Alarm
	Receive Power	Threshold	Threshold	Threshold	Threshold
Port	(dBm)	(dBm)	(dBm)	(dBm)	(dBm)
-----	-----	-----	-----	-----	-----
Gi1/3	N/A ( -0.0) --	-0.0	-0.0	-0.0	-0.0

### Related Commands

Command	Description
<b>switchport access</b>	Configures a port as a static-access or a dynamic-access port.
<b>switchport block</b>	Blocks unknown unicast or multicast traffic on an interface.
<b>switchport backup interface</b>	Configures Flex Links, a pair of Layer 2 interfaces that provide mutual backup.
<b>switchport mode</b>	Configures the VLAN membership mode of a port.
<b>switchport mode private-vlan</b>	Configures a port as a private-VLAN host or a promiscuous port.
<b>switchport private-vlan</b>	Defines private-VLAN association for a host port or private-VLAN mapping for a promiscuous port.
<b>switchport protected</b>	Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch.
<b>switchport trunk pruning</b>	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** [**errors** | **etherchannel** | **protocol status** | **trunk**]

## Syntax Description

<i>interface-id</i>	(Optional) ID of the physical interface, including type, module, and port number.
<b>errors</b>	(Optional) Display error counters.
<b>etherchannel</b>	(Optional) Display EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
<b>protocol status</b>	(Optional) Display status of protocols enabled on interfaces.
<b>trunk</b>	(Optional) Display trunk counters.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.



### Note

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

## 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
Gi1/1          0             0             0             0
Gi1/2          0             0             0             0

<output truncated>
```

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces.

```
Switch# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
```

```
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
FastEthernet1/1: Other, IP, ARP, CDP
FastEthernet1/2: Other, IP
FastEthernet1/3: Other, IP
FastEthernet1/4: Other, IP
FastEthernet1/5: Other, IP
FastEthernet1/6: Other, IP
FastEthernet1/7: Other, IP
FastEthernet1/8: Other, IP
FastEthernet1/9: Other, IP
FastEthernet1/10: Other, IP, CDP
```

<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
Gi1/1          0               0               0
Gi1/2          0               0               0
Gi1/1          80678           4155            0
Gi1/2          82320           126             0
```

<output truncated>

#### Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays additional interface characteristics.

# show interfaces rep

Use the **show interfaces rep** EXEC command to display Resilient Ethernet Protocol (REP) configuration and status for a specified interface or for all interfaces.

**show interfaces** [*interface-id*] **rep** [**detail**]

## Syntax Description

<i>interface-id</i>	(Optional) Display REP configuration and status for a specified physical interface or port channel ID.
<b>detail</b>	(Optional) Display detailed REP configuration and status information.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

In the output for the **show interface rep** [**detail**] command, in addition to an *Open*, *Fail*, or AP (alternate port) state, the Port Role might show as *Fail Logical Open* (*FailLogOpen*) or *Fail No Ext Neighbor* (*FailNoNbr*). These states indicate that the port is physically up, but REP is not configured on the neighboring port. In this case, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. The Port Role for this port shows as *Fail Logical Open*; the port forwards all data traffic on all VLANs. The other failed Port Role shows as *Fail No Ext Neighbor*; this port blocks traffic for all VLANs.

When the external neighbors for the failed ports are configured, the failed ports go through the alternate port state transitions and eventually go to an *Open* state or remain as the alternate port, based on the alternate port election mechanism.

In the **show interfaces rep** command output, ports configured as edge no-neighbors are designated with an asterisk (\*) in front of *Primary Edge* or *Secondary Edge*. In the output of the **show interfaces rep detail** command, *No-Neighbor* is spelled out.

The output of this command is also included in the **show tech-support** privileged EXEC command output.

## Examples

This is sample output from the **show interface rep** command:

```
Switch # show interface rep
Interface              Seg-id  Type           LinkOp  Role
-----
GigabitEthernet 1/1    1       Primary Edge  TWO_WAY  Open
GigabitEthernet 1/2    1       Edge          TWO_WAY  Open
FastEthernet 1/4       2              INIT_DOWN  Fail
```



This is sample output from the **show interface rep** command when the edge port is configured to have no REP neighbor. Note the asterisk (\*) next to *Primary Edge*.

```
Switch# show interface rep
Interface          Seg-id Type          LinkOp  Role
-----
GigabitEthernet1/1 2          TWO_WAY  Open
GigabitEthernet1/2 2      Primary Edge*    TWO_WAY  Open
```

This is sample output from the **show interface rep** command when external neighbors are not configured:

```
Switch # show interface rep
Interface          Seg-id  Type          LinkOp  Role
-----
GigabitEthernet1/1 1          NO_NEIGHBOR FailNoNbr
GigabitEthernet1/2 2          NO_NEIGHBOR FailLogOpen
```

This is sample output from the **show interface rep detail** command for a specified interface:

```
Switch # show interface gigabitethernet1/2 rep detail
GigabitEthernet1/2 REP enabled
Segment-id: 1 (Segment)
PortID: 00030019E85BDD00
Preferred flag: No
Operational Link Status: INIT_DOWN
Current Key: 00000000000000000000
Port Role: Fail
Blocked VLAN: 1-4094
Admin-vlan: 1
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: 1234567890123456
Configured Load-balancing Block VLAN: 1-4094
STCN Propagate to: none
LSL PDU rx: 0, tx: 0
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

## Related Commands

Command	Description
<b>rep segment</b>	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.
<b>show rep topology [detail]</b>	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

# show inventory

Use the **show inventory** EXEC command to display product identification (PID) information for the hardware.

**show inventory** [*entity-name* | **raw**]

## Syntax Description

<i>entity-name</i>	(Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet1/1) into which a small form-factor pluggable (SFP) module is installed.
<b>raw</b>	(Optional) Display every entity in the device.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

The command is case sensitive. With no arguments, the **show inventory** command produces a compact dump of all identifiable entities that have a product identifier. The compact dump displays the entity location (slot identity), entity description, and the unique device identifier (UDI) (PID, VID, and SN) of that entity.



### Note

If there is no PID, no output appears when you enter the **show inventory** command.

## Examples

This is example output from the **show inventory** command:

```
Switch> show inventory
NAME: ''1'', DESCR: ''IE-3000-4TC''
PID: IE-3000-4TC      , VID:      , SN: FHK1152UZRW

NAME: ''IE-3000-4TC - Module in slot 1'', DESCR: ''IE-3000-4TC - Module in slot 1''
PID: 800-28491-01, VID: C1151V545FOC11504, SN: S9FOC115040MRFOC11503J7JF

NAME: ''IEM-3000-8TM - Module in slot 2'', DESCR: ''IEM-3000-8TM - Module in slot 2''
PID: 800-28540-01, VID: C1151V332FOC11515, SN: P0FOC11504ML3

NAME: ''IEM-3000-8FM - Module in slot 3'', DESCR: ''IEM-3000-8FM - Module in slot 3''
PID: 800-28543-01, VID: C1151V462FOC11505, SN: GTFOC11505JMPFOC11505JDX

Switch>
```

# show ip arp inspection

Use the **show ip arp inspection** privileged EXEC command to display the configuration and the operating state of dynamic Address Resolution Protocol (ARP) inspection or the status of this feature for all VLANs or for the specified interface or VLAN.

**show ip arp inspection** [**interfaces** *[interface-id]*] | **log** | **statistics** [**vlan** *vlan-range*] | **vlan** *vlan-range*]

Syntax Description		
<b>interfaces</b> <i>[interface-id]</i>		(Optional) Display the trust state and the rate limit of ARP packets for the specified interface or all interfaces. Valid interfaces include physical ports and port channels.
<b>log</b>		(Optional) Display the configuration and contents of the dynamic ARP inspection log buffer.
<b>statistics</b> [ <b>vlan</b> <i>vlan-range</i> ]		(Optional) Display statistics for forwarded, dropped, MAC validation failure, IP validation failure, access control list (ACL) permitted and denied, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified or if a range is specified, display information only for VLANs with dynamic ARP inspection enabled (active).  You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<b>vlan</b> <i>vlan-range</i>		(Optional) Display the configuration and the operating state of dynamic ARP inspection for the specified VLAN. If no VLANs are specified or if a range is specified, display information only for VLANs with dynamic ARP inspection enabled (active).  You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

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

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Examples** This is an example of output from the **show ip arp inspection** command

Switch# **show ip arp inspection**

```
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled
```

Vlan	Configuration	Operation	ACL Match	Static ACL
----	-----	-----	-----	-----

# show ip arp inspection

1	Enabled	Active	deny-all	No
Vlan	ACL Logging	DHCP Logging	Probe Logging	
----	-----	-----	-----	
1	Acl-Match	All	Permit	
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
----	-----	-----	-----	-----
1	0	0	0	0
Vlan	DHCP Permits	ACL Permits	Probe Permits	Source MAC Failures
----	-----	-----	-----	-----
1	0	0	0	0
Vlan	Dest MAC Failures	IP Validation Failures	Invalid Protocol Data	
----	-----	-----	-----	
1	0	0	0	

This is an example of output from the **show ip arp inspection interfaces** command:

```
Switch# show ip arp inspection interfaces
```

Interface	Trust State	Rate (pps)	Burst Interval
-----	-----	-----	-----
Gi1/1	Untrusted	15	1
Gi1/2	Untrusted	15	1
Gi1/3	Untrusted	15	1

This is an example of output from the **show ip arp inspection interfaces interface-id** command:

```
Switch# show ip arp inspection interfaces gigabitethernet1/1
```

Interface	Trust State	Rate (pps)	Burst Interval
-----	-----	-----	-----
Gi1/1	Untrusted	15	1

This is an example of output from the **show ip arp inspection log** command. It shows the contents of the log buffer before the buffers are cleared:

```
Switch# show ip arp inspection log
```

Total Log Buffer Size : 32

Syslog rate : 10 entries per 300 seconds.

Interface	Vlan	Sender MAC	Sender IP	Num Pkts	Reason	Time
-----	----	-----	-----	-----	-----	----
Gi1/1	5	0003.0000.d673	192.2.10.4	5	DHCP Deny	19:39:01 UTC
Mon Mar 1 1993						
Gi1/1	5	0001.0000.d774	128.1.9.25	6	DHCP Deny	19:39:02 UTC
Mon Mar 1 1993						
Gi1/1	5	0001.c940.1111	10.10.10.1	7	DHCP Deny	19:39:03 UTC
Mon Mar 1 1993						
Gi1/1	5	0001.c940.1112	10.10.10.2	8	DHCP Deny	19:39:04 UTC
Mon Mar 1 1993						
Gi1/1	5	0001.c940.1114	173.1.1.1	10	DHCP Deny	19:39:06 UTC
Mon Mar 1 1993						
Gi1/1	5	0001.c940.1115	173.1.1.2	11	DHCP Deny	19:39:07 UTC
Mon Mar 1 1993						
Gi1/1	5	0001.c940.1116	173.1.1.3	12	DHCP Deny	19:39:08 UTC
Mon Mar 1 1993						

If the log buffer overflows, it means that a log event does not fit into the log buffer, and the display for the **show ip arp inspection log** privileged EXEC command is affected. A -- in the display appears in place of all data except the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer, or increase the logging rate in the **ip arp inspection log-buffer** global configuration command.

This is an example of output from the **show ip arp inspection statistics** command. It shows the statistics for packets that have been processed by dynamic ARP inspection for all active VLANs.

```
Switch# show ip arp inspection statistics
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
-----
5         3              4618         4605            4
2000      0              0            0              0

Vlan      DHCP Permits      ACL Permits      Source MAC Failures
-----
5         0              12              0
2000      0              0              0

Vlan      Dest MAC Failures      IP Validation Failures
-----
5         0              9
2000      0              0
```

For the **show ip arp inspection statistics** command, the switch increments the number of forwarded packets for each ARP request and response packet on a trusted dynamic ARP inspection port. The switch increments the number of ACL or DHCP permitted packets for each packet that is denied by source MAC, destination MAC, or IP validation checks, and the switch increments the appropriate failure count.

This is an example of output from the **show ip arp inspection statistics vlan 5** command. It shows statistics for packets that have been processed by dynamic ARP for VLAN 5.

```
Switch# show ip arp inspection statistics vlan 5
Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
-----
5         3              4618         4605            4

Vlan      DHCP Permits      ACL Permits      Source MAC Failures
-----
5         0              12              0

Vlan      Dest MAC Failures      IP Validation Failures      Invalid Protocol Data
-----
5         0              9              3
```

This is an example of output from the **show ip arp inspection vlan 5** command. It shows the configuration and the operating state of dynamic ARP inspection for VLAN 5.

```
Switch# show ip arp inspection vlan 5
Source Mac Validation      :Enabled
Destination Mac Validation :Enabled
IP Address Validation      :Enabled

Vlan      Configuration      Operation      ACL Match      Static ACL
-----
5         Enabled            Active        second         No

Vlan      ACL Logging      DHCP Logging
-----
5         Acl-Match        All
```

#### Related Commands

Command	Description
<a href="#">arp access-list</a>	Defines an ARP ACL.
<a href="#">clear ip arp inspection log</a>	Clears the dynamic ARP inspection log buffer.
<a href="#">clear ip arp inspection statistics</a>	Clears the dynamic ARP inspection statistics.

Command	Description
<a href="#">ip arp inspection log-buffer</a>	Configures the dynamic ARP inspection logging buffer.
<a href="#">ip arp inspection vlan logging</a>	Controls the type of packets that are logged per VLAN.
<a href="#">show arp access-list</a>	Displays detailed information about ARP access lists.

# show ip dhcp snooping

Use the **show ip dhcp snooping** EXEC command to display the DHCP snooping configuration.

## show ip dhcp snooping

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	Release	Modification
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	Expressions are case sensitive. For example, if you enter <b>exclude output</b> , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
	This command displays only the results of global configuration. Therefore, in this example, the circuit ID suboption appears in its default format of <b>vlan-mod-port</b> , even if a string is configured for the circuit ID.

<b>Examples</b>	This is an example of output from the <b>show ip dhcp snooping</b> command:
-----------------	---

```
Switch> show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
circuit-id format: vlan-mod-port
  remote-id format: string
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
GigabitEthernet1/1       yes         unlimited
GigabitEthernet1/2       yes         unlimited
```

<b>Related Commands</b>	Command	Description
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

# show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** EXEC command to display the DHCP snooping binding database and configuration information for all interfaces on a switch.

**show ip dhcp snooping binding** [*ip-address*] [*mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

## Syntax Description

<i>ip-address</i>	(Optional) Specify the binding entry IP address.
<i>mac-address</i>	(Optional) Specify the binding entry MAC address.
<b>interface</b> <i>interface-id</i>	(Optional) Specify the binding input interface.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specify the binding entry VLAN.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

The **show ip dhcp snooping binding** command output shows only the dynamically configured bindings. Use the **show ip source binding** privileged EXEC command to display the dynamically and statically configured bindings in the DHCP snooping binding database.

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

## Examples

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

```
Switch> show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
01:02:03:04:05:06  10.1.2.150    9837        dhcp-snooping  20    GigabitEthernet1/1
00:D0:B7:1B:35:DE  10.1.2.151    237         dhcp-snooping  20    GigabitEthernet1/2
Total number of bindings: 2
```



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

```
Switch> show ip dhcp snooping binding 10.1.2.150
MacAddress      IPAddress      Lease(sec)    Type           VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9810          dhcp-snooping  20      GigabitEthernet1/1
Total number of bindings: 1
```

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

```
Switch> show ip dhcp snooping binding 0102.0304.0506
MacAddress      IPAddress      Lease(sec)    Type           VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9788          dhcp-snooping  20      GigabitEthernet1/2
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries on a port:

```
Switch> show ip dhcp snooping binding interface gigabitethernet1/2
MacAddress      IPAddress      Lease(sec)    Type           VLAN    Interface
-----
00:30:94:C2:EF:35  10.1.2.151    290           dhcp-snooping  20      GigabitEthernet1/2
Total number of bindings: 1
```


This example shows how to display the DHCP snooping binding entries on VLAN 20:

```
Switch> show ip dhcp snooping binding vlan 20
MacAddress      IPAddress      Lease(sec)    Type           VLAN    Interface
-----
01:02:03:04:05:06  10.1.2.150    9747          dhcp-snooping  20      GigabitEthernet1/1
00:00:00:00:00:02  10.1.2.151    65           dhcp-snooping  20      GigabitEthernet1/2
Total number of bindings: 2
```

Table 2-12 describes the fields in the **show ip dhcp snooping binding** command output:

**Table 2-12** *show ip dhcp snooping binding Command Output*

Field	Description
MacAddress	Client hardware MAC address
IpAddress	Client IP address assigned from the DHCP server
Lease(sec)	Remaining lease time for the IP address
Type	Binding type
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host
Total number of bindings	Total number of bindings configured on the switch
	<b>Note</b> The command output might not show the total number of bindings. For example, if 200 bindings are configured on the switch and you stop the display before all the bindings appear, the total number does not change.

 show ip dhcp snooping binding

Related Commands	Command	Description
	<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.

# show ip dhcp snooping database

Use the **show ip dhcp snooping database** EXEC command to display the status of the DHCP snooping binding database agent.

**show ip dhcp snooping database [detail]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Display detailed status and statistics information.				
<b>Command Modes</b>	EXEC				
<b>Command History</b>	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.2(44)EX</td><td>This command was introduced.</td></tr> </table>	Release	Modification	12.2(44)EX	This command was introduced.
Release	Modification				
12.2(44)EX	This command was introduced.				

## Examples

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

```
Switch> show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
```

```
Total Attempts      :          0   Startup Failures :          0
Successful Transfers :          0   Failed Transfers :          0
Successful Reads     :          0   Failed Reads    :          0
Successful Writes    :          0   Failed Writes   :          0
Media Failures       :          0
```

This is an example of output from the **show ip dhcp snooping database detail** command:

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.
```

```
Total Attempts      :         21   Startup Failures :          0
Successful Transfers :          0   Failed Transfers :         21
Successful Reads     :          0   Failed Reads    :          0
```

**show ip dhcp snooping database**

```

Successful Writes      :      0   Failed Writes      :      21
Media Failures        :      0

First successful access: Read

Last ignored bindings counters :
Binding Collisions      :      0   Expired leases      :      0
Invalid interfaces      :      0   Unsupported vlans :      0
Parse failures          :      0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions      :      0   Expired leases      :      0
Invalid interfaces      :      0   Unsupported vlans :      0
Parse failures          :      0

```

**Related Commands**

Command	Description
<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
<a href="#">ip dhcp snooping database</a>	Configures the DHCP snooping binding database agent or the binding file.
<a href="#">show ip dhcp snooping</a>	Displays DHCP snooping information.

# show ip dhcp snooping statistics

Use the **show ip dhcp snooping statistics** EXEC command to display DHCP snooping statistics in summary or detail form.

**show ip dhcp snooping statistics [detail]**

Syntax Description	detail	(Optional) Display detailed statistics information.
--------------------	--------	---

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

Usage Guidelines	In a switch stack, all statistics are generated on the stack master. If a new stack master is elected, the statistics counters reset.
------------------	---

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

```
Switch> show ip dhcp snooping statistics
Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Switch> show ip dhcp snooping statistics detail
Packets Processed by DHCP Snooping = 0
Packets Dropped Because
  IDB not known                    = 0
  Queue full                       = 0
  Interface is in errdisabled      = 0
  Rate limit exceeded              = 0
  Received on untrusted ports      = 0
  Nonzero giaddr                   = 0
  Source mac not equal to chaddr   = 0
  Binding mismatch                  = 0
  Insertion of opt82 fail          = 0
  Interface Down                   = 0
  Unknown output interface         = 0
  Reply output port equal to input port = 0
  Packet denied by platform        = 0
```

■ `show ip dhcp snooping statistics`

Table 2-13 shows the DHCP snooping statistics and their descriptions:

**Table 2-13 DHCP Snooping Statistics**

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the <b>no ip dhcp snooping information option allow-untrusted</b> global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the <b>ip dhcp snooping verify mac-address</b> global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header.
Insertion of opt82 fail	Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.
Interface Down	Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.
Unknown output interface	Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped.

**Table 2-13**      *DHCP Snooping Statistics (continued)*

DHCP Snooping Statistic	Description
Reply output port equal to input port	Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports.
Packet denied by platform	Number of times the packet has been denied by a platform-specific registry.

Related Commands	Command	Description
	<a href="#">clear ip dhcp snooping</a>	Clears the DHCP snooping binding database, the DHCP snooping binding database agent statistics, or the DHCP snooping statistics counters.

# show ip igmp profile

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

**show ip igmp profile** [*profile number*]

## 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.
-----------------------	---

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## 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** EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN.

**show ip igmp snooping** [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*]

<b>Syntax Description</b>	<b>groups</b>	(Optional) See the <a href="#">show ip igmp snooping groups</a> command.
	<b>mrouter</b>	(Optional) See the <a href="#">show ip igmp snooping mrouter</a> command.
	<b>querier</b>	(Optional) See the <a href="#">show ip igmp snooping querier</a> command.
	<b>vlan</b> <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094 (available only in privileged EXEC mode).

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	Use this command to display snooping configuration for the switch or for a specific VLAN.
	VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

<b>Examples</b>	This is an example of output from the <b>show ip igmp snooping vlan 1</b> command. It shows snooping characteristics for a specific VLAN.
-----------------	---

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----
IGMP snooping                :Enabled
IGMPv3 snooping (minimal)    :Enabled
Report suppression           :Enabled
TCN solicit query            :Disabled
TCN flood query count        :2
Last member query interval   : 100

Vlan 1:
-----
IGMP snooping                :Enabled
Immediate leave               :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode    :IGMP_ONLY
Last member query interval   : 100
```

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

```
Switch> show ip igmp snooping
```

## show ip igmp snooping

```

Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression      : Enabled
TCN solicit query       : Disabled
TCN flood query count    : 2
Last member query interval : 100

Vlan 1:
-----
IGMP snooping           :Enabled
Immediate leave         :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode :IGMP_ONLY
Last member query interval : 100

Vlan 2:
-----
IGMP snooping           :Enabled
Immediate leave         :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode :IGMP_ONLY
Last member query interval : 333

<output truncated>

```

### Related Commands

Command	Description
<b>ip igmp snooping</b>	Enables IGMP snooping on the switch or on a VLAN.
<b>ip igmp snooping last-member-query-interval</b>	Enables the IGMP snooping configurable-leave timer.
<b>ip igmp snooping querier</b>	Enables the IGMP querier function in Layer 2 networks.
<b>ip igmp snooping report-suppression</b>	Enables IGMP report suppression.
<b>ip igmp snooping tcn</b>	Configures the IGMP topology change notification behavior.
<b>ip igmp snooping tcn flood</b>	Specifies multicast flooding as the IGMP spanning-tree topology change notification behavior.
<b>ip igmp snooping vlan immediate-leave</b>	Enables IGMP snooping immediate-leave processing on a VLAN.
<b>ip igmp snooping vlan mrouter</b>	Adds a multicast router port or configures the multicast learning method.
<b>ip igmp snooping vlan static</b>	Statically adds a Layer 2 port as a member of a multicast group.
<b>show ip igmp snooping groups</b>	Displays the IGMP snooping multicast table for the switch.
<b>show ip igmp snooping mrouter</b>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
<b>show ip igmp snooping querier</b>	Displays the configuration and operation information for the IGMP querier configured on a switch.

# show ip igmp snooping groups

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

**show ip igmp snooping groups** [**vlan** *vlan-id* [*ip\_address*] | **dynamic** | *user*] [**count**]

## Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
<i>ip_address</i>	(Optional) Display characteristics of the multicast group with the specified group IP address.
<b>dynamic</b>	(Optional) Display entries learned by IGMP snooping.
<b>user</b>	(Optional) Display only the user-configured multicast entries.
<b>count</b>	(Optional) Display the total number of entries for the specified command options instead of the actual entries.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

Use this command to display multicast information or the multicast table.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

## Examples

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

```
Switch# show ip igmp snooping groups
Vlan      Group      Type      Version    Port List
-----
104       224.1.4.2   igmp      v2         Gi1/1, Gi1/2
104       224.1.4.3   igmp      v2         Gi1/1, Gi1/2
```

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

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

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

```
Switch# show ip igmp snooping groups vlan 1 dynamic
Vlan      Group      Type      Version    Port List
-----
```

## show ip igmp snooping groups

```

104      224.1.4.2      igmp      v2      Gi1/1, Fa1/8
104      224.1.4.3      igmp      v2      Gi1/1, Fa1/8

```

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

```

Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group      Type      Version    Port List
-----
104      224.1.4.2      igmp      v2      Gi1/1, Fa1/8

```

### Related Commands

Command	Description
<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
<a href="#">ip igmp snooping vlan mrouter</a>	Configures a multicast router port.
<a href="#">ip igmp snooping vlan static</a>	Statically adds a Layer 2 port as a member of a multicast group.
<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 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*]

<b>Syntax Description</b>	<b>vlan vlan-id</b> (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

<b>Usage Guidelines</b>	Use this command to display multicast router ports on the switch or for a specific VLAN.
	VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.
	When multicast VLAN registration (MVR) is enabled, the <b>show ip igmp snooping mrouter</b> command displays MVR multicast router information and IGMP snooping information.

<b>Examples</b>	This is an example of output from the <b>show ip igmp snooping mrouter</b> command. It shows how to display multicast router ports on the switch.
-----------------	---

```
Switch# show ip igmp snooping mrouter
Vlan      ports
----      -
1         Gi1/1 (dynamic)
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
	<a href="#">ip igmp snooping vlan mrouter</a>	Adds a multicast router port.
	<a href="#">ip igmp snooping vlan static</a>	Statically adds a Layer 2 port as a member of a multicast group.
	<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN
	<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information for the switch or for the specified parameter.

# show ip igmp snooping querier

Use the **show ip igmp snooping querier detail** EXEC command to display the configuration and operation information for the IGMP querier configured on a switch.

**show ip igmp snooping querier** [**detail** | **vlan** *vlan-id* [**detail**]]

Syntax Description	<b>detail</b>	Optional) Display detailed IGMP querier information.
	<b>vlan</b> <i>vlan-id</i> [ <b>detail</b> ]	Optional) Display IGMP querier information for the specified VLAN. The range is 1 to 1001 and 1006 to 4094. Use the <b>detail</b> keyword to display detailed information.

Command Modes	EXEC
---------------	------

Command History	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

**Usage Guidelines**

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a *querier*, that sends IGMP query messages. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router*. If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

The **show ip igmp snooping querier detail** EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the switch querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the switch querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the switch querier (if any) that is configured in the VLAN

**Examples**

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

```
Switch> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11    v3                 Gi1/1
2         172.20.40.20    v2                 Router
```

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

```
Switch> show ip igmp snooping querier detail
```

```

Vlan      IP Address      IGMP Version  Port
-----
1         1.1.1.1         v2           Fa1/1

Global IGMP switch querier status
-----
admin state           : Enabled
admin version         : 2
source IP address     : 0.0.0.0
query-interval (sec)  : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10

Vlan 1:  IGMP switch querier status

-----
elected querier is 1.1.1.1      on port Fa1/1
-----
admin state           : Enabled
admin version         : 2
source IP address     : 10.1.1.65
query-interval (sec)  : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10
operational state     : Non-Querier
operational version    : 2
tcn query pending count : 0

```

Related Commands	Command	Description
	<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
	<a href="#">ip igmp snooping querier</a>	Enables the IGMP querier function in Layer 2 networks.
	<a href="#">show ip igmp snooping</a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

# show ip source binding

Use the **show ip source binding** EXEC command to display the IP source bindings on the switch.

**show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**interface** *interface-id*] [**vlan** *vlan-id*]

## Syntax Description

<i>ip-address</i>	(Optional) Display IP source bindings for a specific IP address.
<i>mac-address</i>	(Optional) Display IP source bindings for a specific MAC address.
<b>dhcp-snooping</b>	(Optional) Display IP source bindings that were learned by DHCP snooping.
<b>static</b>	(Optional) Display static IP source bindings.
<b>interface</b> <i>interface-id</i>	(Optional) Display IP source bindings on a specific interface.
<b>vlan</b> <i>vlan-id</i>	(Optional) Display IP source bindings on a specific VLAN.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

The **show ip source binding** command output shows the dynamically and statically configured bindings in the DHCP snooping binding database. Use the **show ip dhcp snooping binding** privileged EXEC command to display only the dynamically configured bindings.

## Examples

This is an example of output from the **show ip source binding** command:

```
Switch> show ip source binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:00:00:0A:00:0B  11.0.0.1      infinite    static         10    GigabitEthernet1/1
00:00:00:0A:00:0A  11.0.0.2      10000       dhcp-snooping  10    GigabitEthernet1/1
```

## Related Commands

Command	Description
<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database.
<a href="#">ip source binding</a>	Configures static IP source bindings on the switch.



# show ip verify source

Use the **show ip verify source** EXEC command to display the IP source guard configuration on the switch or on a specific interface.

**show ip verify source** [**interface** *interface-id*]

<b>Syntax Description</b>	<b>interface</b> <i>interface-id</i> (Optional) Display IP source guard configuration on a specific interface.
---------------------------	--

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

## Examples

This is an example of output from the **show ip verify source** command:

```
Switch> show ip verify source
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
-----
gi1/1     ip           active       10.0.0.1    10
gi1/1     ip           active       deny-all   11-20
gi1/2     ip           inactive-trust-port
gi1/3     ip           inactive-no-snooping-vlan
gi1/4     ip-mac       active       10.0.0.2    aaaa.bbbb.cccc 10
gi1/4     ip-mac       active       11.0.0.1    aaaa.bbbb.cccc 11
gi1/4     ip-mac       active       deny-all   deny-all      12-20
gi1/5     ip-mac       active       10.0.0.3    permit-all    10
gi1/5     ip-mac       active       deny-all   permit-all    11-20
```

In the previous example, this is the IP source guard configuration:

- On the Gigabit Ethernet 1 interface, DHCP snooping is enabled on VLANs 10 to 20. For VLAN 10, IP source guard with IP address filtering is configured on the interface, and a binding exists on the interface. For VLANs 11 to 20, the second entry shows that a default port access control lists (ACLs) is applied on the interface for the VLANs on which IP source guard is not configured.
- The Gigabit Ethernet 2 interface is configured as trusted for DHCP snooping.
- On the Gigabit Ethernet 3 interface, DHCP snooping is not enabled on the VLANs to which the interface belongs.
- On the Gigabit Ethernet 4 interface, IP source guard with source IP and MAC address filtering is enabled, and static IP source bindings are configured on VLANs 10 and 11. For VLANs 12 to 20, the default port ACL is applied on the interface for the VLANs on which IP source guard is not configured.
- On the Gigabit Ethernet 5 interface, IP source guard with source IP and MAC address filtering is enabled and configured with a static IP binding, but port security is disabled. The switch cannot filter source MAC addresses.

This is an example of output on an interface on which IP source guard is disabled:

```
Switch> show ip verify source gigabitethernet 1/6
```

 `show ip verify source`

IP source guard is not configured on the interface gil1/16.

**Related Commands**

Command	Description
<a href="#">ip verify source</a>	Enables IP source guard on an interface.

# show ipc

Use the **show ipc** EXEC command to display Interprocess Communications Protocol (IPC) configuration, status, and statistics.

```
show ipc {hog-info | mcast {appclass | groups | status} | nodes | ports [open] | queue | rpc |
        session {all | rx | tx} [verbose] | status [cumulative] | zones}
```

## Syntax Description

<b>mcast</b> { <b>appclass</b>   <b>groups</b>   <b>status</b> }	Display the IPC multicast routing information. The keywords have these meanings: <ul style="list-style-type: none"> <li><b>appclass</b>—Display the IPC multicast application classes.</li> <li><b>groups</b>—Display the IPC multicast groups.</li> <li><b>status</b>—Display the IPC multicast routing status.</li> </ul>
<b>nodes</b>	Display participating nodes.
<b>ports</b> [ <b>open</b> ]	Display local IPC ports. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>open</b>—(Optional) Display only the open ports.</li> </ul>
<b>queue</b>	Display the contents of the IPC transmission queue.
<b>rpc</b>	Display the IPC remote-procedure statistics.
<b>session</b> { <b>all</b>   <b>rx</b>   <b>tx</b> }	Display the IPC session statistics (available only in privileged EXEC mode). The keywords have these meanings: <ul style="list-style-type: none"> <li><b>all</b>—Display all the session statistics.</li> <li><b>rx</b>—Display the sessions statistics for traffic that the switch receives</li> <li><b>tx</b>—Display the sessions statistics for traffic that the switch forwards.</li> </ul>
<b>verbose</b>	(Optional) Display detailed statistics (available only in privileged EXEC mode).
<b>status</b> [ <b>cumulative</b> ]	Display the status of the local IPC server. The keyword has this meaning: <ul style="list-style-type: none"> <li><b>cumulative</b>—(Optional) Display the status of the local IPC server since the switch was started or restarted.</li> </ul>
<b>zones</b>	Display the participating IPC zones. The switch supports a single IPC zone.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Usage Guidelines

This command is available only when the switch is running the IP Services image.

## Examples

This example shows how to display the IPC routing status:

```
Switch> show ipc mcast status
```

```

                                IPC Mcast Status
                                Tx          Rx
Total Frames                    0          0
Total control Frames            0          0
Total Frames dropped            0          0
Total control Frames dropped    0          0

Total Reliable messages        0          0
Total Reliable messages acknowledged 0          0
Total Out of Band Messages    0          0
Total Out of Band messages acknowledged 0          0

Total No Mcast groups          0          0

Total Retries                   0  Total Timeouts                0
Total OOB Retries               0  Total OOB Timeouts            0
Total flushes                   0  Total No ports              0

```

This example shows how to display the participating nodes:

```

Switch> show ipc nodes
There is 1 node in this IPC realm.
  ID      Type      Name              Last Sent  Last Heard
  10000 Local      IPC Master        0         0

```

This example shows how to display the local IPC ports:

```

Switch> show ipc ports
There are 8 ports defined.

Port ID      Type      Name                                     (current/peak/total)
There are 8 ports defined.
  10000.1      unicast  IPC Master:Zone
  10000.2      unicast  IPC Master:Echo
  10000.3      unicast  IPC Master:Control
  10000.4      unicast  IPC Master:Init
  10000.5      unicast  FIB Master:DFS.process_level.msgs
  10000.6      unicast  FIB Master:DFS.interrupt.msgs
  10000.7      unicast  MDFS RP:Statistics
    port_index = 0  seat_id = 0x10000  last sent = 0  last heard = 0
0/2/159

  10000.8      unicast  Slot 1 :MDFS.control.RIL
    port_index = 0  seat_id = 0x10000  last sent = 0  last heard = 0
0/0/0

RPC packets:current/peak/total
                                           0/1/4

```

This example shows how to display the contents of the IPC retransmission queue:

```

Switch> show ipc queue
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 IPC messages waiting for a response.
There are 0 IPC messages waiting for additional fragments.
There are 0 IPC messages currently on the IPC inboundQ.
Messages currently in use                :      3
Message cache size                      :    1000
Maximum message cache usage              :    1000

0 times message cache crossed            5000 [max]

Emergency messages currently in use      :      0

```

There are 2 messages currently reserved for reply msg.

Inbound message queue depth 0  
Zone inbound message queue depth 0

This example shows how to display all the IPC session statistics:

Switch# **show ipc session all**

Tx Sessions:

Port ID	Type	Name	port_index	type	last sent	last heard
10000.7	Unicast	MDFS RP:Statistics	0	Unreliable	0	0
Msgs requested = 180 Msgs returned = 180						
10000.8	Unicast	Slot 1 :MDFS.control.RIL	0	Reliable	0	0
Msgs requested = 0 Msgs returned = 0						

Rx Sessions:

Port ID	Type	Name	port_index	seat_id	last sent	last heard
10000.7	Unicast	MDFS RP:Statistics	0	0x10000	0	0
No of msgs requested = 180 Msgs returned = 180						
10000.8	Unicast	Slot 1 :MDFS.control.RIL	0	0x10000	0	0
No of msgs requested = 0 Msgs returned = 0						

This example shows how to display the status of the local IPC server:

Switch> **show ipc status cumulative**

IPC System Status

Time last IPC stat cleared :never

This processor is the IPC master server.  
Do not drop output of IPC frames for test purposes.

1000 IPC Message Headers Cached.

	Rx Side	Tx Side
Total Frames	12916	608
0	0	
Total from Local Ports	13080	574
Total Protocol Control Frames	116	17
Total Frames Dropped	0	0

Service Usage

Total via Unreliable Connection-Less Service	12783	171
Total via Unreliable Sequenced Connection-Less Svc	0	0
Total via Reliable Connection-Oriented Service	17	116

<output truncated>

## Related Commands

Command	Description
<b>clear ipc</b>	Clears the IPC multicast routing statistics.

# show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in EXEC mode.

**show ipv6 access-list** [*access-list-name*]

## Syntax Description

*access-list-name* (Optional) Specifies the name of access list.

## Command Modes

EXEC (>)

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.



### Note

This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch and the switch is running the IP Services image.

## Examples

The following output from the **show ipv6 access-list** command shows IPv6 access lists named inbound and outbound:

```
Router# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30
```

[Table 2-14](#) describes the significant fields shown in the display.

**Table 2-14 show ipv6 access-list Field Descriptions**

Field	Description
IPv6 access list inbound	Name of the IPv6 access list, for example, inbound.
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.

**Table 2-14** *show ipv6 access-list Field Descriptions (continued)*

Field	Description
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.
bgp (matches)	Border Gateway Protocol. The protocol type that the packet is equal to and the number of matches.
sequence 10	Sequence in which an incoming packet is compared to lines in an access list. Access list lines are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).

#### Related Commands

Command	Description
<b>clear ipv6 access-list</b>	Resets the IPv6 access list match counters.
<b>ipv6 access-list</b>	Defines an IPv6 access list and puts the switch into IPv6 access-list configuration mode.
<b>sdm prefer</b>	Configures an SDM template to optimize system resources based on how the switch is being used.

# show ipv6 dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the **show ipv6 dhcp conflict** command in privileged EXEC mode.

**show ipv6 dhcp conflict**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

---

<b>Command History</b>	Release	Modification
	12.2(52)SE	This command was introduced.

---

---

<b>Usage Guidelines</b>	<p>This command is available only if the switch is running the IP Services image and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template. To configure the dual IPv4 and IPv6 template, enter the <b>sdm prefer dual-ipv4-and-ipv6</b> global configuration command, and reload the switch.</p>
-------------------------	--

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

---

<b>Examples</b>	This is an example of the output from the <b>show ipv6 dhcp conflict</b> command:
-----------------	---

```
Switch# show ipv6 dhcp conflict
Pool 350, prefix 2001:1005::/48
      2001:1005::10
```

---

<b>Related Commands</b>	Command	Description
	<a href="#">ipv6 dhcp pool</a>	Configures a DHCPv6 pool and enters DHCPv6 pool configuration mode.
	<a href="#">clear ipv6 dhcp conflict</a>	Clears an address conflict from the DHCPv6 server database.

---



# show ipv6 mld snooping

To display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN, use the **show ipv6 mld snooping** command in EXEC mode.

**show ipv6 mld snooping** [*vlan vlan-id*]

Syntax Description	<i>vlan vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
--------------------	---------------------	---

Command Modes	EXEC (>)
---------------	----------

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

Usage Guidelines	Use this command to display MLD snooping configuration for the switch or for a specific VLAN.
------------------	---



## Note

This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples	This is an example of output from the <b>show ipv6 mld snooping vlan</b> command. It shows snooping characteristics for a specific VLAN.
----------	--

```
Switch> show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-----
MLD snooping                : Enabled
MLDv2 snooping (minimal)    : Enabled
Listener message suppression : Enabled
TCN solicit query           : Disabled
TCN flood query count       : 2
Robustness variable         : 3
Last listener query count    : 2
Last listener query interval : 1000
Vlan 100:
-----
MLD snooping                : Disabled
MLDv1 immediate leave       : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable         : 3
Last listener query count    : 2
Last listener query interval : 1000
```

This is an example of output from the **show ipv6 mld snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Switch> show ipv6 mld snooping
Global MLD Snooping configuration:
-----
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

#### Related Commands

Command	Description
<a href="#">ipv6 mld snooping</a>	Enables and configures MLD snooping on the switch or on a VLAN.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.

# show ipv6 mld snooping address

To display all or specified IP version 6 (IPv6) multicast address information maintained by Multicast Listener Discovery (MLD) snooping, use the **show ipv6 mld snooping address** command in EXEC mode.

**show ipv6 mld snooping address** [[**vlan** *vlan-id*] [*ipv6-multicast-address*]] [**vlan** *vlan-id*] [**count** | **dynamic** | **user**]

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies a VLAN about which to show MLD snooping multicast address information. The VLAN ID range is 1 to 1001 and 1006 to 4094.
	<i>ipv6-multicast-address</i>	(Optional) Displays information about the specified IPv6 multicast address. This keyword is only available when a VLAN ID is entered.
	<b>count</b>	(Optional) Displays the number of multicast groups on the switch or in the specified VLAN.
	<b>dynamic</b>	(Optional) Displays MLD snooping learned group information.
	<b>user</b>	(Optional) Displays MLD snooping user-configured group information.

**Command Modes** EXEC (>)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SE	This command was introduced.

**Usage Guidelines** Use this command to display IPv6 multicast address information.



## Note

This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

You can enter an IPv6 multicast address only after you enter a VLAN ID.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Use the **dynamic** keyword to display information only about groups that are learned. Use the **user** keyword to display information only about groups that have been configured.

**Examples** This is an example of output from the **show ipv6 mld snooping address** EXEC command:

```
Switch> show ipv6 mld snooping address
Vlan Group   Type Version Port List
-----
2    FF12:::3 user          Fa1/2, Gi1/2, Gi1/1,Gi1/3
```

**show ipv6 mld snooping address**

This is an example of output from the **show ipv6 mld snooping address count EXEC** command:

```
Switch> show ipv6 mld snooping address count
Total number of multicast groups: 2
```

This is an example of output from the **show ipv6 mld snooping address EXEC** command:

```
Switch> show ipv6 mld snooping address user
Vlan Group  Type Version Port List
-----
2          FF12::3 user   v2      Fa1/2, Gi1/2, Gi1/1,Gi1/3
```

**Related Commands**

Command	Description
<a href="#">ipv6 mld snooping vlan</a>	Configures IPv6 MLD snooping on a VLAN.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.

# show ipv6 mld snooping mrouter

To display dynamically learned and manually configured IP version 6 (IPv6) Multicast Listener Discovery (MLD) router ports for the switch or a VLAN, use the **show ipv6 mld snooping mrouter** command in EXEC mode.

**show ipv6 mld snooping mrouter** [*vlan vlan-id*]

Syntax Description	<i>vlan vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
--------------------	---------------------	---

Command Modes	EXEC (>)
---------------	----------

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

Usage Guidelines	Use this command to display MLD snooping router ports for the switch or for a specific VLAN.
------------------	--

**Note**

This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.


VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples	This is an example of output from the <b>show ipv6 mld snooping mrouter</b> command. It displays snooping characteristics for all VLANs on the switch that are participating in MLD snooping.
----------	---

```
Switch> show ipv6 mld snooping mrouter
Vlan      ports
----      -
    2      Gi1/11 (dynamic)
   72      Gi1/11 (dynamic)
  200      Gi1/11 (dynamic)
```

This is an example of output from the **show ipv6 mld snooping mrouter vlan** command. It shows multicast router ports for a specific VLAN.

```
Switch> show ipv6 mld snooping mrouter vlan 100
Vlan      ports
----      -
    2      Gi1/11 (dynamic)
```

 show ipv6 mld snooping mrouter

Related Commands	Command	Description
	<b>ipv6 mld snooping</b>	Enables and configures MLD snooping on the switch or on a VLAN.
	<b>ipv6 mld snooping vlan mrouter</b> <b>interface</b> <i>interface-id</i>   <b>static</b> <i>ipv6-multicast-address</i> <b>interface</b> <i>interface-id</i> ]	Configures multicast router ports for a VLAN.
	<b>sdm prefer</b>	Configures an SDM template to optimize system resources based on how the switch is being used.

# show ipv6 mld snooping querier

To display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping querier-related information most recently received by the switch or the VLAN, use the **show ipv6 mld snooping querier** command in EXEC mode.

**show ipv6 mld snooping querier** [**vlan** *vlan-id*] [**detail**]

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
	<b>detail</b>	(Optional) Displays detailed MLD snooping querier information for the switch or for the VLAN.

<b>Command Modes</b>	EXEC (>)
----------------------	----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SE	This command was introduced.

**Usage Guidelines** Use the **show ipv6 mld snooping querier** command to display the MLD version and IPv6 address of a detected device that sends MLD query messages, which is also called a *querier*. A subnet can have multiple multicast routers but has only one MLD querier. The querier can be a Layer 3 switch.



## Note

This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

The **show ipv6 mld snooping querier** command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router*. If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

The output of the **show ipv6 mld snoop querier vlan** command displays the information received in response to a query message from an external or internal querier. It does not display user-configured VLAN values, such as the snooping robustness variable on the particular VLAN. This querier information is used only on the MASQ message that is sent by the switch. It does not override the user-configured robustness variable that is used for aging out a member that does not respond to query messages.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

## Examples

This is an example of output from the **show ipv6 mld snooping querier** command:

```
Switch> show ipv6 mld snooping querier
Vlan      IP Address      MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1          Gi1/1
```

This is an example of output from the **show ipv6 mld snooping querier detail** command:

```
Switch> show ipv6 mld snooping querier detail
Vlan      IP Address      MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1      Gi1/1
```

This is an example of output from the **show ipv6 mld snooping querier vlan** command:

```
Switch> show ipv6 mld snooping querier vlan 2
IP address : FE80::201:C9FF:FE40:6000
MLD version : v1
Port : Gi1/1
Max response time : 1000s
```

#### Related Commands

Command	Description
<a href="#">ipv6 mld snooping</a>	Enables and configures IPv6 MLD snooping on the switch or on a VLAN.
<a href="#">ipv6 mld snooping last-listener-query-count</a>	Configures the maximum number of queries that the switch sends before aging out an MLD client.
<a href="#">ipv6 mld snooping last-listener-query-interval</a>	Configures the maximum response time after sending out a query that the switch waits before deleting a port from the multicast group.
<a href="#">ipv6 mld snooping robustness-variable</a>	Configures the maximum number of queries that the switch sends before aging out a multicast address when there is no response.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<a href="#">ipv6 mld snooping</a>	Enables and configures IPv6 MLD snooping on the switch or on a VLAN.



# show ipv6 route updated

To display the current contents of the IPv6 routing table, use the **show ipv6 route updated** command in privileged EXEC mode.

```
show ipv6 route [protocol] updated [boot-up]{hh:mm | day{month [hh:mm]} [{hh:mm | day{month [hh:mm]}]}
```

Syntax Description		
	<i>protocol</i>	(Optional) Displays routes for the specified routing protocol using any of these keywords: <ul style="list-style-type: none"> <li><b>bgp</b></li> <li><b>isis</b></li> <li><b>ospf</b></li> <li><b>rip</b></li> </ul> Displays routes for the specified type of route using any of these keywords: <ul style="list-style-type: none"> <li><b>connected</b></li> <li><b>local</b></li> <li><b>static</b></li> <li><b>interface</b> <i>interface id</i></li> </ul>
	<b>boot-up</b>	(Optional) Displays the current contents of the IPv6 routing table.
	<i>hh:mm</i>	The time as a 2-digit number for a 24-hour clock. Make sure to use the colons (:). For example, enter <b>13:32</b> .
	<i>day</i>	The day of the month. The range is from 1 to 31.
	<i>month</i>	The month in uppercase or lowercase letters. You can enter the full name of the month, such as <b>January</b> or <b>august</b> , or the first three letters of the month, such as <b>jan</b> or <b>Aug</b> .

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.2(46)SE1	This command was introduced.

**Usage Guidelines** Use the **show ipv6 route updated** privileged EXEC command to display the current contents of the IPv6 routing table.



## Note

This command is available only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

**Examples**

This is an example of output from the **show ipv6 route updated rip** command:

```
Switch> show ipv6 route rip updated
IPv6 Routing Table - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
IA - ISIS interarea, IS - ISIS summary
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R 2001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:8D01, GigabitEthernet1/1
Last updated 10:31:10 27 February 2007
R 2004::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/2
Last updated 17:23:05 22 February 2007
R 4000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/3
Last updated 17:23:05 22 February 2007
R 5000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/4
Last updated 17:23:05 22 February 2007
R 5001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/5
Last updated 17:23:05 22 February 2007
```

**Related Commands**

Command	Description
<b>show ipv6 route</b>	Displays the current contents of the IPv6 routing table. For syntax information, see the <i>Cisco IOS Software Command Reference, Release 15.0</i> .

# show l2protocol-tunnel

To display information about Layer 2 protocol tunnel ports, use the **show l2protocol-tunnel** command in EXEC mode.

**show l2protocol-tunnel** [**interface** *interface-id*] [**summary**] ]

## Syntax Description

<b>interface</b> <i>interface-id</i>	(Optional) Specifies the interface for which protocol tunneling information appears. Valid interfaces are physical ports and port channels; the port channel range is 1 to 48.
<b>summary</b>	(Optional) Displays only summary information about Layer 2 protocol tunnel ports.

## Command Modes

EXEC (>)

## Command History

Release	Modification
12.2(52)SE	This command was introduced.

## Usage Guidelines

You must first enable Layer 2 protocol tunneling on an access or IEEE 802.1Q tunnel port by using the **l2protocol-tunnel** command in interface configuration mode. You then can configure some or all of these parameters:

- Protocol type to be tunneled
- Shutdown threshold
- Drop threshold

If you enter the **show l2protocol-tunnel** [**interface** *interface-id*] command, only information about the active ports on which all the parameters are configured appears.

If you enter the **show l2protocol-tunnel summary** command, only information about the active ports on which some or all of the parameters are configured appears.



### Note

This command is available only when the switch is running the IP Services image.

**Examples**

This is an example of output from the **show l2protocol-tunnel** command:

```
Switch> show l2protocol-tunnel
```

```
COS for Encapsulated Packets: 5
```

```
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Fa1/3	---	----	----	----	----	----
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	----	0	242500	
	lacp	----	----	24268	242640	
Fa1/4	udld	----	----	0	897960	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	24249	242700	
	lacp	----	----	24256	242660	
Gi1/3	udld	----	----	0	897960	
	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	0	242500	
Gi1/4	lacp	500	----	0	485320	
	udld	300	----	44899	448980	
	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	1000	0	242700	
	lacp	----	----	0	485220	
	udld	300	----	44899	448980	

This is an example of output from the **show l2protocol-tunnel summary** command:

```
Switch> show l2protocol-tunnel summary
```

```
COS for Encapsulated Packets: 5
```

```
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Drop Threshold (cdp/stp/vtp) (pagp/lacp/udld)	Status
Fa1/2	---	----/----/----	----/----/----	up
	pagp lacp udld	----/----/----	----/----/----	
Fa1/3	---	----/----/----	----/----/----	up
	pagp lacp udld	1000/----/----	----/----/----	
Fa1/4	---	----/----/----	----/----/----	up
	pagp lacp udld	1000/ 500/----	----/----/----	
Fa1/5	cdp stp vtp	----/----/----	----/----/----	down
	---	----/----/----	----/----/----	
Gi1/1	---	----/----/----	----/----/----	down
	pagp	----/----/----	1000/----/----	
Gi1/2	---	----/----/----	----/----/----	down
	pagp	----/----/----	1000/----/----	

**Related Commands**

Command	Description
<a href="#">clear l2protocol-tunnel counters</a>	Clears counters for protocol tunneling ports.
<a href="#">l2protocol-tunnel</a>	Enables Layer 2 protocol tunneling for CDP, STP, or VTP packets on an interface.
<a href="#">l2protocol-tunnel cos</a>	Configures a class of service (CoS) value for tunneled Layer 2 protocol packets.

# show lacp

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

**show lacp** [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**}

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to .
<b>counters</b>	Display traffic information.
<b>internal</b>	Display internal information.
<b>neighbor</b>	Display neighbor information.
<b>sys-id</b>	Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the switch MAC address.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

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

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

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

## Examples

This is an example of output from the **show lacp counters** EXEC command. [Table 2-15](#) describes the fields in the display.

```
Switch> show lacp counters
          LACPDUs      Marker      Marker Response      LACPDUs
Port      Sent   Recv      Sent   Recv      Sent   Recv      Pkts Err
-----
Channel group:1
Gi1/1      19     10         0       0         0       0         0
Gi1/2      14      6         0       0         0       0         0
```

**Table 2-15** *show lacp counters* Field Descriptions

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.

**Table 2-15** *show lacp counters Field Descriptions (continued)*

Field	Description
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDU's Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

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

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

Channel group 1

Port      Flags   State   LACP port   Admin   Oper   Port   Port
          State Priority Key       Key     Number State
Gi1/1     SA      bndl    32768       0x3     0x3    0x4    0x3D
Gi1/2     SA      bndl    32768       0x3     0x3    0x5    0x3D
```

Table 2-16 describes the fields in the display:

**Table 2-16** *show lacp internal Field Descriptions*

Field	Description
State	State of the specific port. These are the allowed values: <ul style="list-style-type: none"> <li>—Port is in an unknown state.</li> <li><b>bndl</b>—Port is attached to an aggregator and bundled with other ports.</li> <li><b>susp</b>—Port is in a suspended state; it is not attached to any aggregator.</li> <li><b>hot-sby</b>—Port is in a hot-standby state.</li> <li><b>indiv</b>—Port is incapable of bundling with any other port.</li> <li><b>indep</b>—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).</li> <li><b>down</b>—Port is down.</li> </ul>
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.

**Table 2-16** *show lacp internal Field Descriptions (continued)*

Field	Description
Port Number	Port number.
Port State	<p>State variables for the port, encoded as individual bits within a single octet with these meanings:</p> <ul style="list-style-type: none"> <li>• bit0: LACP_Activity</li> <li>• bit1: LACP_Timeout</li> <li>• bit2: Aggregation</li> <li>• bit3: Synchronization</li> <li>• bit4: Collecting</li> <li>• bit5: Distributing</li> <li>• bit6: Defaulted</li> <li>• bit7: Expired</li> </ul> <p><b>Note</b> In the list above, bit7 is the MSB and bit0 is the LSB.</p>

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

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

Channel group 3 neighbors

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi1/1	32768,0007.eb49.5e80	0xC	19s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi1/2	32768,0007.eb49.5e80	0xD	15s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

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

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

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



Related Commands	Command	Description
	<a href="#">clear lacp</a>	Clears the LACP channel-group information.
	<a href="#">lacp port-priority</a>	Configures the LACP port priority.
	<a href="#">lacp system-priority</a>	Configures the LACP system priority.

# show location

Use the **show location** EXEC command to display location information for an endpoint.

```
show location [admin-tag] [civic-location | elin-location { cdp | identifier id | interface
interface-id | static}]
```

Syntax Description	<b>admin-tag</b>	(Optional) Display administrative tag or site information.
	<b>civic-location</b>	(Optional) Display civic location information.
	<b>elin-location</b>	(Optional) Display emergency location information (ELIN).
	<b>cdp</b>	(Optional) Display CDP location information.
	<b>identifier id</b>	(Optional) Specify the ID for the civic location or the elin location. The id range is 1 to 4095.
	<b>interface interface-id</b>	(Optional) Display location information for the specified interface or all interfaces. Valid interfaces include physical ports.
	<b>static</b>	(Optional) Display static configuration information.

Command Modes	EXEC
---------------	------

Command History	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

Usage Guidelines	Use the <b>show location</b> command to display location information for an endpoint.
------------------	---

Examples	This is an example of output from the <b>show location civic-location</b> command that displays location information for an interface:
----------	--

```
Switch> show location civic interface gigabitethernet1/1
Civic location information
-----
Identifier           : 1
County              : Santa Clara
Street number       : 3550
Building            : 19
Room                : C6
Primary road name   : Cisco Way
City                : San Jose
State               : CA
Country             : US
```

This is an example of output from the **show location civic-location** command that displays all the civic location information:

```
Switch> show location civic-location static
Civic location information
-----
```

```

Identifier          : 1
County             : Santa Clara
Street number      : 3550
Building           : 19
Room               : C6
Primary road name   : Cisco Way
City               : San Jose
State              : CA
Country            : US
Ports              : Gil/1
-----
Identifier          : 2
Street number      : 24568
Street number suffix : West
Landmark           : Golden Gate Bridge
Primary road name   : 19th Ave
City               : San Francisco
Country            : US
-----

```

This is an example of output from the **show location elin-location** command that displays the emergency location information:

```

Switch> show location elin-location identifier 1
Elin location information
-----
Identifier : 1
Elin       : 14085553881
Ports      : Gil/2

```

This is an example of output from the **show location elin static** command that displays all emergency location information:

```

Switch> show location elin static
Elin location information
-----
Identifier : 1
Elin       : 14085553881
Ports      : Gil/2
-----
Identifier : 2
Elin       : 18002228999
-----

```

## Related Commands

Command	Description
<a href="#">location (global configuration)</a>	Configures the global location information for an endpoint.
<a href="#">location (interface configuration)</a>	Configures the location information for an interface.

# show link state group

Use the **show link state group** privileged EXEC command to display the link-state group information.

**show link state group** [*number*] [**detail**]

<b>Syntax Description</b>	<i>number</i>	(Optional) Number of the link-state group.
	<b>detail</b>	(Optional) Specify that detailed information appears.

**Defaults** There is no default.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

**Usage Guidelines** Use the **show link state group** command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group.

Enter the **detail** keyword to display detailed information about the group. The output for the **show link state group detail** command displays only those link-state groups that have link-state tracking enabled or that have upstream or downstream interfaces (or both) configured. If there is no link-state group configuration for a group, it is not shown as enabled or disabled.

**Examples** This is an example of output from the **show link state group 1** command:

```
Switch> show link state group 1
Link State Group: 1      Status: Enabled, Down
```

This is an example of output from the **show link state group detail** command:

```
Switch> show link state group detail
(Up):Interface up      (Dwn):Interface Down      (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi1/1(Dwn) Gi1/2(Dwn)
Downstream Interfaces : Fa1/5(Dis) Fa1/6(Dis) Fa1/7(Dis) Fa1/8(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi1/1(Dwn) Gi1/2(Dwn) Gi1/3(Dwn)
Downstream Interfaces : Fa1/5(Dis) Fa1/6(Dis) Fa1/7(Dis) Fa1/8(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Commands	Command	Description
	<a href="#">link state group</a>	Configures an interface as a member of a link-state group.
	<a href="#">link state track</a>	Enables a link-state group.

# show mac access-group

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

**show mac access-group**

## Syntax Description

<b>interface</b> <i>interface-id</i>	(Optional) Display the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port-channel range is 1 to 6 (available only in privileged EXEC mode).
--------------------------------------	---

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Examples

This is an example of output from the **show mac-access group** EXEC command. Port 2 has the MAC access list *macl\_e1* applied; no MAC ACLs are applied to other interfaces.

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

<output truncated>

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

```
Switch# show mac access-group interface gigabitethernet1/1
Interface GigabitEthernet1/1:
  Inbound access-list is macl_e1
```

## Related Commands

Command	Description
<a href="#">mac access-group</a>	Applies a MAC access group to an interface.

# show mac address-table

Use the **show mac address-table** 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**

## Syntax Description

**Command Modes** EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

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

## Examples

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

```
Switch> show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
A11     0000.0000.0001   STATIC    CPU
A11     0000.0000.0002   STATIC    CPU
A11     0000.0000.0003   STATIC    CPU
A11     0000.0000.0009   STATIC    CPU
A11     0000.0000.0012   STATIC    CPU
A11     0180.c200.000b   STATIC    CPU
A11     0180.c200.000c   STATIC    CPU
A11     0180.c200.000d   STATIC    CPU
A11     0180.c200.000e   STATIC    CPU
A11     0180.c200.000f   STATIC    CPU
A11     0180.c200.0010   STATIC    CPU
1       0030.9441.6327   DYNAMIC    Gi1/2
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 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** 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** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

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

```
Switch# show mac address-table address 0002.4b28.c482
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0002.4b28.c482  STATIC  CPU
Total Mac Addresses for this criterion: 1
```

Related Commands	Command	Description
	<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 aging-time

Use the **show mac address-table aging-time** 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	EXEC
---------------	------

Command History	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

Usage Guidelines	<p>If no VLAN number is specified, the aging time for all VLANs appears.</p> <p>Expressions are case sensitive. For example, if you enter   <b>exclude output</b>, the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.</p>
------------------	---

Examples	This is an example of output from the <b>show mac address-table aging-time</b> 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
```

## ■ show mac address-table aging-time

Related Commands	Command	Description
	<b>mac address-table aging-time</b>	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
	<b>show mac address-table address</b>	Displays MAC address table information for the specified MAC address.
	<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 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 count

Use the **show mac address-table count** 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

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

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

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

## Examples

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

```
Switch# show mac address-table count
Mac Entries for Vlan   : 1
-----
Dynamic Address Count  : 2
Static Address Count   : 0
Total Mac Addresses    : 2
```

Related Commands	Command	Description
	<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 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 dynamic

Use the **show mac address-table dynamic** 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 <i>interfaces</i> 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	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

Examples	This is an example of output from the <b>show mac address-table dynamic</b> command:
----------	--

```
Switch> show mac address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0030.b635.7862   DYNAMIC Gi1/2
1       00b0.6496.2741   DYNAMIC Gi1/2
Total Mac Addresses for this criterion: 2
```

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 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 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	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

Examples	This is an example of output from the <b>show mac address-table interface</b> command:
----------	--

```
Switch> show mac address-table interface gigabitethernet1/2
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0030.b635.7862   DYNAMIC Gi1/2
1       00b0.6496.2741   DYNAMIC Gi1/2
Total Mac Addresses for this criterion: 2
```

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 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 learning

Use the **show mac address-table learning** EXEC command to display the status of MAC address learning for all VLANs or the specified VLAN.

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

<b>Syntax Description</b>	<b>vlan</b> <i>vlan-id</i>	(Optional) Display 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.

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(46)SE1	This command was introduced.

**Usage Guidelines**

Use the **show mac address-table learning** command without any keywords to display configured VLANs and whether MAC address learning is enabled or disabled on them. The default is that MAC address learning is enabled on all VLANs. Use the command with a specific VLAN ID to display the learning status on an individual VLAN.

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

**Examples**

This is an example of output from the **show mac address-table learning** EXEC command showing that MAC address learning is disabled on VLAN 200:

```
Switch> show mac address-table learning
VLAN      Learning Status
----      -
1          yes
100        yes
200        no
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">mac address-table learning vlan</a>	Enables or disables MAC address learning on a VLAN.

# show mac address-table move update

Use the **show mac address-table move update** EXEC command to display the MAC address-table move update information on the switch.

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

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

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

Examples	This is an example of output from the <b>show mac address-table move update</b> command:
----------	--

```
Switch> show mac address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
switch#
```

Related Commands	Command	Description
	<a href="#">clear mac address-table move update</a>	Clears the MAC address-table move update counters.
	<a href="#">mac address-table move update {receive   transmit}</a>	Configures MAC address-table move update on the switch.

# show mac address-table notification

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

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

Syntax Description		
<b>change</b>		Display the MAC change notification feature parameters and the history table.
<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>mac-move</b>		Display status for MAC address move notifications.
<b>threshold</b>		Display status for MAC-address table threshold monitoring.
<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	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

**Usage Guidelines**

Use the **show mac address-table notification change** command without keywords to see if the MAC address change notification 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 notifications for all interfaces. If the *interface-id* is included, only the flags for that interface appear.

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

**Examples**

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

```
Switch> show mac address-table notification change
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>mac address-table notification</b>	Enables the MAC address notification feature for MAC address changes, moves, or address-table thresholds.
<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 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** EXEC command to display only static MAC address table entries.

```
show mac address-table static [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 <i>interfaces</i> include physical ports and port channels.
<b>vlan</b> <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

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

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



**Examples**

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

```
Switch> show mac address-table static
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0100.0ccc.cccc   STATIC  CPU
All     0180.c200.0000   STATIC  CPU
All     0100.0ccc.cccd   STATIC  CPU
All     0180.c200.0001   STATIC  CPU
All     0180.c200.0004   STATIC  CPU
All     0180.c200.0005   STATIC  CPU
4       0001.0002.0004   STATIC  Drop
6       0001.0002.0007   STATIC  Drop
Total Mac Addresses for this criterion: 8
```

**Related Commands**

Command	Description
<b>mac address-table static</b>	Adds static addresses to the MAC address table.
<b>mac address-table static drop</b>	Enables unicast MAC address filtering and configures the switch to drop traffic with a specific source or destination MAC address.
<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 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** 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

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

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

## Examples

This is an example of output from the **show 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.c200.0005   STATIC  CPU
1       0180.c200.0006   STATIC  CPU
1       0180.c200.0007   STATIC  CPU
Total Mac Addresses for this criterion: 9
```

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 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** 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	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

Examples	This is an example of output from the <b>show mls qos</b> command when QoS is enabled and DSCP transparency is enabled:
----------	---

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

Related Commands	Command	Description
	<a href="#">mls qos</a>	Enables QoS for the entire switch.

# show mls qos aggregate-policer

Use the **show mls qos aggregate-policer 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	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

Examples	This is an example of output from the <b>show mls qos aggregate-policer</b> command:
----------	--

```
Switch> show mls qos aggregate-policer policer1
aggregate-policer policer1 1000000 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** 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	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

Examples	This is an example of output from the <b>show mls qos input-queue</b> command:
----------	--

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

Related Commands	Command	Description
	<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** EXEC command to display quality of service (QoS) information at the port 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 port. 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 **policer** keyword is not supported.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

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

## Examples

This is an example of output from the **show mls qos interface** *interface-id* command when VLAN-based QoS is enabled:

```
Switch> show mls qos interface gigabitethernet1/1
GigabitEthernet1/1
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
```



```
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:vlan-based
```

This is an example of output from the **show mls qos interface *interface-id*** command when VLAN-based QoS is disabled:

```
Switch> show mls qos interface gigabitethernet1/2
GigabitEthernet1/2
trust state:not trusted
trust mode:not trusted
trust enabled flag:ena
COS override:dis
default COS:0
DSCP Mutation Map:Default DSCP Mutation Map
Trust device:none
qos mode:port-based
```

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

```
Switch> show mls qos interface gigabitethernet1/2 buffers
GigabitEthernet1/2
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 *interface-id* queueing** command. The egress expedite queue overrides the configured shaped round robin (SRR) weights.

```
Switch> show mls qos interface gigabitethernet1/2 queueing
GigabitEthernet1/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) : 25 0 0 0
Shared queue weights : 25 25 25 25
The port bandwidth limit : 100 (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

This is an example of output from the **show mls qos interface *interface-id* statistics** command. [Table 2-17](#) describes the fields in this display.

```
Switch> show mls qos interface gigabitethernet1/2 statistics
GigabitEthernet1/2
```

```
      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
```

# show mls qos interface

```

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
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 packets received for each DSCP value.
	outgoing	Number of packets sent for each DSCP value.
CoS	incoming	Number of packets received for each CoS value.
	outgoing	Number of packets sent 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 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.

Command	Description
<b>mls qos srr-queue output dscp-map</b>	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<b>policy-map</b>	Creates or modifies a policy map.
<b>priority-queue</b>	Enables the egress expedite queue on a port.
<b>queue-set</b>	Maps a port to a queue-set.
<b>srr-queue bandwidth limit</b>	Limits the maximum output on a port.
<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.

# show mls qos maps

Use the **show mls qos maps** 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.

<b>Command Modes</b>	EXEC
----------------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

The policed-DSCP, DSCP-to-CoS, and the DSCP-to-DSCP-mutation maps appear 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 appear 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 02-01 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 01-01 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

```

# show mls qos maps

```

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 02-01 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
<b>mls qos map</b>	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.
<b>mls qos srr-queue input cos-map</b>	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
<b>mls qos srr-queue input dscp-map</b>	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
<b>mls qos srr-queue output cos-map</b>	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
<b>mls qos srr-queue output dscp-map</b>	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 EXEC** command to display quality of service (QoS) settings for the egress queues.

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

<b>Syntax Description</b>	<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.


<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

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

<b>Examples</b>	This is an example of output from the <b>show mls qos queue-set</b> command:
-----------------	--

```
Switch> show mls qos queue-set
Queueset: 1
Queue   :      1      2      3      4
-----
buffers  :      25     25     25     25
threshold1:    100    200    100    100
threshold2:    100    200    100    100
reserved  :      50     50     50     50
maximum  :     400    400    400    400
Queueset: 2
Queue   :      1      2      3      4
-----
buffers  :      25     25     25     25
threshold1:    100    200    100    100
threshold2:    100    200    100    100
reserved  :      50     50     50     50
maximum  :     400    400    400    400
```

 show mls qos queue-set

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 mls qos vlan

Use the **show mls qos vlan** EXEC command to display the policy maps attached to a switch virtual interface (SVI).

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

## Syntax Description

<i>vlan-id</i>	Specify the VLAN ID of the SVI to display the policy maps. 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

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

The output from the **show mls qos vlan** command is meaningful only when VLAN-based quality of service (QoS) is enabled and when hierarchical policy maps are configured.

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

## Examples

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

```
Switch> show mls qos vlan 10
Vlan10
Attached policy-map for Ingress:pm-test-pm-2
```

## Related Commands

Command	Description
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports and enters policy-map configuration mode.

# show monitor

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

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

## Syntax Description

<b>session</b>	(Optional) Display information about specified SPAN sessions.
<b>session_number</b>	Specify the number of the SPAN or RSPAN session. The range is 1 to 66.
<b>all</b>	Display all SPAN sessions.
<b>local</b>	Display only local SPAN sessions.
<b>range</b> <i>list</i>	Display a range of SPAN sessions, where <i>list</i> is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.  <b>Note</b> This keyword is available only in privileged EXEC mode.
<b>remote</b>	Display only remote SPAN sessions.
<b>detail</b>	(Optional) Display detailed information about the specified 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

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

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

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 EXEC** command:

```
Switch# show monitor
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Fa1/1
Both : Fa2/2-3,Fa2/5-6
Destination Ports : Fa1/2
Encapsulation : Replicate
Ingress : Disabled

Session 2
-----
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

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

```
Switch# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Fa1/1
Both : Fa2/2-3,Fa2/5-6
Destination Ports : Fa2/8
Encapsulation : Replicate
Ingress : Disabled
```

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

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

Session 2
-----
Type : Local Session
Source Ports :
Both : Fa1/5
Destination Ports : Fa1/8
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

## 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
	12.2(44)EX	This command was introduced.

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

Examples	This is an example of output from the <b>show mvr</b> 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 interoperability 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, 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
12.2(44)EX	This command was 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 appear. If you enter a VLAN ID, all MVR group members in the VLAN appear.

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

## Examples

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

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

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** command for a specified port:

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

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

```
Switch# show mvr interface gigabitethernet1/2 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
<b>mvr (global configuration)</b>	Enables and configures multicast VLAN registration on the switch.
<b>mvr (interface configuration)</b>	Configures MVR ports.
<b>show mvr</b>	Displays the global MVR configuration on the switch.
<b>show mvr members</b>	Displays all receiver ports that are members of an MVR multicast group.

# show mvr members

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

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

## Syntax Description

<i>ip-address</i>	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as 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
12.2(44)EX	This command was introduced.

## Usage Guidelines

The **show mvr members** command applies to receiver and source ports. For MVR-compatible mode, all source ports are members of all multicast groups.

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

## Examples

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

```
Switch# show mvr members
MVR Group IP      Status      Members
-----
239.255.0.1      ACTIVE      Gil1/1(d), Gil2(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>
```



This is an example of output from the **show mvr members** *ip-address* command. It displays the members of the IP multicast group with that address:

```
Switch# show mvr members 239.255.0.2
239.255.003.--22      ACTIVE      Gi1/1(d), Gi1/2(d), Gi1/3(d),
                               Gi1/4(d), Gi1/5(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 network-policy profile

Use the **show network-policy profile** privileged EXEC command to display the network-policy profiles.

**show network-policy profile** [*profile number*] [**detail**] [ | { **begin** | **exclude** | **include** } *expression*]



## Note

To use this command, the switch must be running the LAN Base image.

## Syntax Description

<i>profile number</i>	(Optional) Display the network-policy profile number. If no profile is entered, all network-policy profiles appear.
<b>detail</b>	(Optional) Display detailed status and statistics 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

Privileged EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Examples

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

```
Switch# show network-policy profile
Network Policy Profile 10
  voice vlan 17 cos 4
  Interface:
    none
Network Policy Profile 30
  voice vlan 30 cos 5
  Interface:
    none
Network Policy Profile 36
  voice vlan 4 cos 3
  Interface:
    Interface_id
```

## Related Commands

Command	Description
<a href="#">network-policy</a>	Applies a network-policy to an interface.

Command	Description
<a href="#">network-policy profile (global configuration)</a>	Creates the network-policy profile.
<a href="#">network-policy profile (network-policy configuration)</a>	Configures the attributes of network-policy profiles.

# show nmosp

Use the **show nmosp** privileged EXEC command to display the Network Mobility Services Protocol (NMSP) information for the switch. This command is available only when your switch is running the cryptographic (encrypted) software image.

```
show nmosp {attachment suppress interface | capability | notification interval | statistics
            {connection | summary} | status | subscription {detail | summary}} [ | {begin | exclude |
            include} expression]
```

Syntax Description		
<b>attachment suppress interface</b>		Display attachment suppress interfaces.
<b>capability</b>		Display switch capabilities including the supported services and subservices.
<b>notification interval</b>		Display the notification intervals of the supported services.
<b>statistics {connection   summary}</b>		Display the NMSP statistics information. <ul style="list-style-type: none"> <li>• <b>connection</b>—display the message counters on each connection.</li> <li>• <b>summary</b>—display the global counters.</li> </ul>
<b>status</b>		Display information about the NMSP connections.
<b>subscription {detail   summary}</b>		Display the subscription information on each NMSP connection. <ul style="list-style-type: none"> <li>• <b>detail</b>—display all services and subservices subscribed on each connection.</li> <li>• <b>summary</b>—display all services subscribed on each connection.</li> </ul>
<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.

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Examples** This is an example of output from the **show nmosp attachment suppress interface** command:

```
Switch# show nmosp attachment suppress interface
NMSP Attachment Suppression Interfaces
-----
GigabitEthernet1/1
GigabitEthernet1/2
```

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

```
Switch# show nmsp capability
NMSP Switch Capability
-----
Service           Subservice
-----
Attachment        Wired Station
Location           Subscription
```

This is an example of output from the **show nmsp notification interval** command:

```
Switch# show nmsp notification interval
NMSP Notification Intervals
-----
Attachment notify interval: 30 sec (default)
Location notify interval: 30 sec (default)
```

This is an example of output from the **show nmsp statistics connection** and **show nmsp statistics summary** commands:

```
Switch# show nmsp statistics connection
NMSP Connection Counters
-----
Connection 1:
  Connection status: UP
  Freed connection: 0

  Tx message count      Rx message count
  -----
  Subscr Resp: 1        Subscr Req: 1
  Capa Notif: 1         Capa Notif: 1
  Atta Resp: 1          Atta Req: 1
  Atta Notif: 0
  Loc Resp: 1           Loc Req: 1
  Loc Notif: 0
  Unsupported msg: 0

Switch# show nmsp statistics summary
NMSP Global Counters
-----
  Send too big msg: 0
  Failed socket write: 0
  Partial socket write: 0
  Socket write would block: 0
  Failed socket read: 0
  Socket read would block: 0
  Transmit Q full: 0
  Max Location Notify Msg: 0
  Max Attachment Notify Msg: 0
  Max Tx Q Size: 0
```

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

```
Switch# show nmsp status
NMSP Status
-----
NMSP: enabled
MSE IP Address      TxEchoResp RxEchoReq TxData RxData
172.19.35.109       5 5 4 4
```

This is an example of output from the **show nmsp show subscription detail** and the **show nmsp show subscription summary** commands:

```
Switch# show nmsp subscription detail
Mobility Services Subscribed by 172.19.35.109:
Services                Subservices
-----
Attachment:            Wired Station
Location:               Subscription

Switch# show nmsp subscription summary
Mobility Services Subscribed:
MSE IP Address          Services
-----
172.19.35.109           Attachment, Location
```

#### Related Commands

Command	Description
<a href="#">clear nmsp statistics</a>	Clears the NMSP statistic counters.
<a href="#">nmsp</a>	Enables Network Mobility Services Protocol (NMSP) on the switch.

# show pagp

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

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

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to 6.
<b>counters</b>	Display traffic information.
<b>dual-active</b>	Display the dual-active status.
<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

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.
12.2(46)SE	The <b>dual-active</b> keyword was added.

## 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* do not appear, but the lines that contain *Output* are appear.

## Examples

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

```
Switch> show pagp 1 counters
              Information          Flush
Port          Sent   Recv          Sent   Recv
-----
Channel group: 1
Gi1/1         45     42           0       0
Gi1/2         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.
```

**show pagp**

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
Gi1/1	SC	U6/S7	H	30s	1	128	Any	16
Gi1/2	SC	U6/S7	H	30s	1	128	Any	16

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

Switch> **show pagp 1 neighbor**

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

Channel group 1 neighbors

Port	Partner Name	Partner Device ID	Partner Port	Partner Age	Partner Flags	Partner Group Cap.
Gi1/1	switch-p2	0002.4b29.4600	Gi0/1	9s	SC	10001
Gi1/2	switch-p2	0002.4b29.4600	Gi0/2	24s	SC	10001

This is an example of output from the **show pagp dual-active** command:

Switch> **show pagp dual-active**

PAGP dual-active detection enabled: Yes

PAGP dual-active version: 1.1

Channel group 1

Port	Dual-Active Detect Capable	Partner Name	Partner Port	Partner Version
Gi1/1	No	Switch	Gi1/3	N/A

<output truncated>

**Related Commands**

Command	Description
<a href="#">clear pagp</a>	Clears PAGP channel-group information.



# show parser macro

Use the **show parser macro EXEC** command to display the parameters for all configured macros or for one macro on the switch.

**show parser macro** [{**brief** | **description** [**interface** *interface-id*] | **name** *macro-name*}] [ | {**begin** | **exclude** | **include**} *expression*]

Syntax Description	
<b>brief</b>	(Optional) Display the name of each macro.
<b>description</b> [ <b>interface</b> <i>interface-id</i> ]	(Optional) Display all macro descriptions or the description of a specific interface.
<b>name</b> <i>macro-name</i>	(Optional) Display information about a single macro identified by the macro 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	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.
	12.2(46)SE1	New macros is optimized for industrial automation traffic were introduced.

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

Examples	This is a partial output example from the <b>show parser macro</b> command. The output for the Cisco-default macros varies depending on the switch platform and the software image running on the switch:
----------	---

```
Switch# show parser macro
<output truncated>

Macro name : cisco-ie-global
Macro type : default global
#global macro name cisco-ie-global macro
#macro description cisco-ie-global
# Access List and Policy May for CIP QoS
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
```

```
access-list 107 permit udp any eq 320 any
```

```
class-map match-all CIP-Implicit_dscp_55
  match access-group 101
class-map match-all CIP-Implicit_dscp_47
  match access-group 102
class-map match-all CIP-Implicit_dscp_43
  match access-group 103
class-map match-all CIP-Implicit_dscp_any
  match access-group 104
class-map match-all CIP-Other
  match access-group 105
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all 1588-PTP-General
  match access-group 107
<output truncated>
```

```
-----
Macro name : cisco-ethernetip
Macro type : default interface
#macro keywords $access_vlan
#macro name cisco-ethernetip
#macro description cisco-ethernetip
switchport host
switchport access vlan $access_vlan
storm-control broadcast level 3.00 1.00
service-policy input CIP-PTP-Traffic
priority-queue out
srr-queue bandwidth share 1 19 40 40
<output truncated>
-----
```

```
Macro name : cisco-ie-desktop
Macro type : default interface
# macro keywords $access_vlan
#macro name cisco-ie-desktop
switchport mode access
switchport access vlan $access_vlan
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 2
switchport port-security violation restrict
no switchport port-security aging type inactivity
no switchport access vlan
no switchport mode access
no spanning-tree portfast
no spanning-tree bpduguard enable
no macro description
-----
```

```
Macro name : cisco-ie-switch
Macro type : default interface
# macro keywords $native_vlan
#macro name: cisco-ie-switch
switchport mode trunk
switchport trunk native vlan $native_vlan
spanning-tree link-type point-to-point
mls qos trust cos
service-policy input CIP-PTP-Traffic
priority-queue out
srr-queue bandwidth share 1 19 40 40
no macro description
macro description cisco-ie-switch
<output truncated>
```

This is an example of output from the **show parser macro name** command:

```
Switch# show parser macro name standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

This is an example of output from the **show parser macro brief** command:

```
Switch# show parser macro brief
<output truncated>
    default global      : cisco-ie-global
    default interface: cisco-ethernetip
    default interface: cisco-ie-desktop
    default interface: cisco-ie-switch
    default interface: cisco-ie-router
    default interface: cisco-ie-phone
    default interface: cisco-ie-wireless
Switch#
```

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

```
Switch# show parser macro description
Global Macro(s): cisco-global
Interface      Macro Description(s)
-----
Gi1/1          standard-switch10
Gi1/2          this is test macro
-----
```

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

```
Switch# show parser macro description interface gigabitethernet1/2
Interface      Macro Description
-----
Gi1/2          this is test macro
-----
```

## Related Commands

Command	Description
<a href="#">macro apply</a>	Applies a macro on an interface or applies and traces a macro on an interface.
<a href="#">macro description</a>	Adds a description about the macros that are applied to an interface.
<a href="#">macro global</a>	Applies a macro on a switch or applies and traces a macro on a switch.
<a href="#">macro global description</a>	Adds a description about the macros that are applied to the switch.
<a href="#">macro name</a>	Creates a macro.
<a href="#">show running-config</a>	Displays the current operating configuration, including defined macros. For syntax information, select <b>Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 &gt; File Management Commands &gt; Configuration File Management Commands</b> .

# show policy-map

Use the **show policy-map 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 **control-plane** and **interface** keywords are not supported, and the statistics shown in the display should be ignored.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

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

## Examples

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

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

Policy Map mypolicy
  class dscp5
    set dscp 6
```

Related Commands	Command	Description
	<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

# show port-security

Use the **show port-security** privileged EXEC command to display port-security settings for an interface or for the switch.

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

## Syntax Description

<b>interface</b> <i>interface-id</i>	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, module, and port number).
<b>address</b>	(Optional) Display all secure MAC addresses on all ports or a specified port.
<b>vlan</b>	(Optional) Display port security settings for all VLANs on the specified interface. This keyword is visible only on interfaces that have the switchport mode set to <b>trunk</b> .
<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
12.2(44)EX	This command was 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 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 command displays all the MAC addresses for the interface with aging information for each secure address. You can also use this command to display all the MAC addresses for an interface even if you have not enabled port security on it.

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

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

## 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)
-----
      Gi1/1      1          0          0          Shutdown
-----
Total Addresses in System (excluding one mac per port)      : 1
Max Addresses limit in System (excluding one mac per port) : 6272

```

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

```

Switch# show port-security interface gigabitethernet1/1
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    Gi1/2     1
-----

Total Addresses in System (excluding one mac per port)      : 1
Max Addresses limit in System (excluding one mac per port) : 6272

```

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

```

Switch# show port-security interface gigabitethernet1/2 address

Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
      1    0006.0700.0800   SecureConfigured    Gi1/2     1
-----

Total Addresses: 1


```

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

```

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

```

 show port-security

Related Commands	Command	Description
	<a href="#">clear port-security</a>	Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface.
	<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 profinet

Use the **show profinet** EXEC command to display information about the PROFINET sessions on the switch.

**show profinet** { **alarm** | **lldp** | **session** | **status** } [ | { **begin** | **exclude** | **include** } *expression* ]

Syntax Description		
<b>alarm</b>		Display PROFINET alarms.
<b>lldp</b>		Display PROFINET Link Layer Discovery Protocol (LLDP).
<b>session</b>		Display PROFINET sessions.
<b>status</b>		Display PROFINET 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	EXEC
---------------	------

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

Usage Guidelines	<p>When LLDP and PROFINET are enabled, this command shows the physical ports that are sending and receiving PROFINET-formatted LLDP packets.</p> <p>Expressions are case sensitive. For example, if you enter <b>  exclude output</b>, the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.</p>
------------------	--

Examples	This example shows how to display PROFINET alarms:
----------	--

```
Switch> show profinet alarm
Monitoring of Profinet Switch Alarms
  RPS Alarm: -
  CF Alarm: -
  Primary Temperature Alarm: -
  Secondary Temperature Alarm: -
  Major Relay Alarm: -
  Minor Relay Alarm: -
Monitoring of Profinet Port Alarms
Port    Link Fault    Not Forwarding    Not Operating    FCS Error
Fa1/1   -             -                 -               -
Fa1/2   -             -                 -               -
Fa1/3   -             -                 -               -
Fa1/4   -             -                 -               -
Fa1/5   -             -                 -               -
Fa1/6   -             -                 -               -
Fa1/7   -             -                 -               -
Fa1/8   -             -                 -               -
```

```

Gi1/1  -          -          -          -
Gi1/2  -          -          -          -

```

This example shows how to display PROFINET LLDP:

```

Switch> show profinet lldp
Fa1/1  port-003      Off
Fa1/2  port-004      Off
Fa1/3  port-005      Off
Fa1/4  port-006      Off
Fa1/5  port-007      Off
Fa1/6  port-008      Off
Fa1/7  port-009      Off
Fa1/8  port-010      Off
Gi1/1  port-001      Off
Gi1/2  port-002      Off
Switch>

```

This example shows how to display a PROFINET session:

```

Switch> show profinet session
Session #1
-----
Connected: No
Number Of IO CR's: 0
Number Of DiffModules: 0

```

This example shows how to display the PROFINET status:

```

Switch> show profinet status
State      : Enabled
Vlan       : 1
Id         : IE3000-8TC
Connected  : Yes
ReductRatio : 512
GSD version : Match

```

## Related Commands

Command	Description
<a href="#">debug profinet alarm</a>	Enables debugging of the PROFINET alarms.
<a href="#">debug profinet cyclic</a>	Displays the function calls related to sending and receiving PROFINET cyclic packets.
<a href="#">debug profinet error</a>	Enables debugging of the PROFINET session errors.
<a href="#">debug profinet packet</a>	Enables debugging of the PROFINET packets.
<a href="#">debug profinet platform</a>	Enables debugging of the interaction between the Cisco IOS software and PROFINET.
<a href="#">debug profinet topology</a>	Displays the received PROFINET topology packets.
<a href="#">debug profinet trace</a>	Displays a group of traced debug output logs.
<a href="#">profinet</a>	Enables the PROFINET feature on the switch.
<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

# show psp config

To display the status of protocol storm protection configured for a specific protocol on a VLAN, use the **show psp config** privileged EXEC command.

**show psp config {arp | dhcp | igmp}**

## Syntax Description

<b>arp</b>	Show protocol storm protection status for ARP and ARP snooping.
<b>dhcp</b>	Show protocol storm protection status for DHCP and DHCP snooping.
<b>igmp</b>	Show protocol storm protection status for IGMP and IGMP snooping.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(58)SE	This command was introduced.

## Examples

This is an example of output from the **show psp config dhcp** command with protocol storm protection configured to drop packets when the incoming rate exceeds 35 packets per second.

```
Switch# show psp config dhcp
```

```
-----  
PSP Protocol Configuration Summary:  
-----
```

```
DHCP Rate Limit      : 35 packets/sec  
PSP Action           : Packet Drop
```

## Related Commands

Command	Description
<b>psp {arp   dhcp   igmp} pps <i>value</i></b>	Configures protocol storm protection for ARP, DHCP, or IGMP.
<b>show psp statistics</b>	Displays the number of dropped packets when protocol storm protection is configured.
<b>clear psp counter</b>	Clears the counter of dropped packets.

# show psp statistics

To display the number of packets dropped for all protocols when protocol storm protection is configured, use the **show psp statistics** privileged EXEC command.

**show psp statistics [arp | dhcp | igmp]**

## Syntax Description

<b>arp</b>	(Optional) Show the number of packets dropped for ARP and ARP snooping.
<b>dhcp</b>	(Optional) Show the number of packets dropped for DHCP and DHCP snooping.
<b>igmp</b>	(Optional) Show the number of packets dropped for IGMP and IGMP snooping.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(58)SE	This command was introduced.

## Examples

This is an example of output from the **show psp statistics dhcp** command when protocol storm protection is configured for DHCP. The output shows that 13 packets were dropped.

```
Switch# show psp statistics dhcp

-----
PSP Protocol Drop Counter Summary:
-----
DHCP Drop Counter: 13
```

## Related Commands

Command	Description
<b>psp {arp   dhcp   igmp} pps value</b>	Configures protocol storm protection for ARP, DHCP, or IGMP.
<b>show psp config</b>	Displays the protocol storm protection configuration.
<b>clear psp counter</b>	Clears the counter of dropped packets.

# show ptp

To view the Precision Time Protocol (PTP) properties that are configured on the port, use the **show ptp** privileged EXEC command.

**show ptp** { **clock** | **foreign-master-record** | **parent** | **port** [**FastEthernet interface** | **GigabitEthernet interface**] | **time-property** | **passthrough** }

Syntax Description	
<b>clock</b>	Displays the PTP clock properties.
<b>foreign-master-record</b>	Displays the foreign master data set.
<b>parent</b>	Displays the parent and grandmaster properties.
<b>port</b>	Displays the PTP port properties.
<b>FastEthernet interface</b>	(Optional) Displays the PTP FastEthernet properties on the specified port.
<b>GigabitEthernet interface</b>	(Optional) Displays the PTP Gigabit Ethernet properties on the specified port.
<b>time-property</b>	Displays the PTP time properties.
<b>passthrough</b>	Displays the PTP pass-through status.

**Defaults** There are no defaults.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(46)SE1	This command was introduced.
	12.2(58)SE	The <b>passthrough</b> keyword was added.

**Usage Guidelines** The **show ptp foreign-master-record** and **show ptp parent** commands apply to boundary clock mode, even though the commands also appear in end-to-end transparent mode.

If you enter the **show ptp clock** or **show ptp port** privileged EXEC command when the switch is in PTP forward mode, an error message states that no information is available.

**Examples** This is an example of output from the **show ptp clock** command:

```
Switch# show ptp clock
PTP CLOCK INFO
  PTP Device Type: Boundary clock
  Clock Identity: 0x0:9:B7:FF:FE:FF:F3:0
  Clock Domain: 0
  Number of PTP ports: 10
  Priority1: 128
  Priority2: 128
  Clock Quality:
    Class: 248
```

```

    Accuracy: Unknown
    Offset (log variance): N/A
Offset From Master: 0
Mean Path Delay: 490
Steps Removed: 1
Local clock time: 18:49:38 UTC Mar 7 1993

```

This is an example of output from the **show ptp port FastEthernet 1/1** command:

```

Switch# show ptp port FastEthernet 1/1
PTP PORT DATASET: FastEthernet1/1
  Port identity: clock identity: 0x0:9:B7:FF:FE:FF:F3:0
  Port identity: port number: 1
  PTP version: 2
  Port state: SLAVE
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay: 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 50000

```

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

```

Switch# show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
    Parent Clock Identity: 0x0:1E:13:FF:FE:0:28:0
    Parent Port Number: 1
    Observed Parent Offset (log variance): N/A
    Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
    Grandmaster Clock Identity: 0x0:1E:13:FF:FE:0:28:0
    Grandmaster Clock Quality:
      Class: 248
      Accuracy: Unknown
      Offset (log variance): N/A
      Priority1: 127
      Priority2: 128

```

This is an example of output from the **show ptp time-property** command:

```

Switch# show ptp time-property
PTP CLOCK TIME PROPERTY:
  Current UTC Offset valid: 0
  Current UTC Offset: 0
  Leap59: 0
  Leap61: 0
  Time Traceable: 16
  Frequency Traceable: 32
  PTP Timescale: 1
  Time Source: Internal Oscillator

```

This is an example of output from the **show ptp foreign-master-record** command:

```

Switch# show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
Interface FastEthernet1/1
  Foreign Master Clock Identity: FF:EE:DD:FF:FE:CC:BB:AA
  Foreign Master Port Number: 4
  Number of Announce Messages: 3
  Message Received Port: 1

```

```
Most Recent Time stamps: 73097688078005270, 73097687836293940
Interface FastEthernet1/2
Empty
Interface FastEthernet1/3
Empty
Interface FastEthernet1/4
Empty
Interface GigabitEthernet1/1
Empty
Interface GigabitEthernet1/2
Foreign Master Clock Identity: 00:09:B7:FF:FE:FF:7D:80
Foreign Master Port Num: 6
Number of Announce messages: 3
Message received port: 6
Most Recent Time stamps: 73097687967991270, 73097687725402960
```

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

```
Switch# show ptp passthrough
PTP Passthrough Enabled
Switch#
```

#### Related Commands

Command	Description
<a href="#">ptp (interface configuration)</a>	Sets the PTP clock properties.
<a href="#">ptp (interface configuration)</a>	Sets the PTP clock properties on a port.
<a href="#">debug ptp</a>	Enables debugging of PTP activity.

# show rep topology

Use the **show rep topology** EXEC command to display Resilient Ethernet Protocol (REP) topology information for a segment or for all segments, including the primary and secondary edge ports in the segment.

**show rep topology** [*segment segment\_id*] [**archive**] [**detail**] [ | { **begin** | **exclude** | **include** } *expression*]

## Syntax Description

<i>segment-id</i>	(Optional) Display REP topology information for the specified segment. The ID range is from 1 to 1024.
<b>archive</b>	(Optional) Display the previous topology of the segment. This keyword can be useful for troubleshooting a link failure.
<b>detail</b>	(Optional) Display detailed REP topology 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

EXEC

## Command History

Release	Modification
12.2(50)SE	This command was introduced.

## Usage Guidelines

In the **show rep topology** command output, ports configured as edge no-neighbor are designated with an asterisk (\*) in front of *Pri* or *Sec*. In the output of the **show rep topology detail** command, *No-Neighbor* is spelled out.

The output of this command is also included in the **show tech-support** privileged EXEC command output.

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 sample output from the **show rep topology segment** privileged EXEC command:

```
Switch # show rep topology segment 1
REP Segment 1
BridgeName      PortName      Edge Role
-----
sw1_multseg_3750 Gi1/1/1      Pri  Alt
sw3_multseg_3400 Gi1/13              Open
sw3_multseg_3400 Gi1/14              Alt
sw4_multseg_3400 Gi0/13              Open
sw4_multseg_3400 Gi0/14              Open
sw5_multseg_3400 Gi1/13              Open
```



```
sw5_multseg_3400 Gi1/14      Open
sw2_multseg_3750 Gi1/0/2     Open
sw2_multseg_3750 Gi1/0/1     Open
sw1_multseg_3750 Gi1/0/2     Sec Open
```

This is a sample output from the **show rep topology** command when the edge ports are configured to have no REP neighbor:

```
Switch # show rep topology
REP Segment 2
BridgeName      PortName      Edge  Role
-----
sw8-ts8-51      Gi1/2          Pri*  Open
sw9-ts11-50     Gi1/0/4        Open
sw9-ts11-50     Gi1/0/2        Open
sw1-ts11-45     Gi0/2          Alt
sw1-ts11-45     Po1            Open
sw8-ts8-51      Gi1/1          Sec*  Open
```

This example shows output from the **show rep topology detail** command:

```
Switch# show rep topology detail
REP Segment 2
repc_2_24ts, Fa0/2 (Primary Edge)
  Alternate Port, some vlans blocked
  Bridge MAC: 0019.e714.5380
  Port Number: 004
  Port Priority: 080
  Neighbor Number: 1 / [-10]
repc_3_12cs, Gi1/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 001
  Port Priority: 000
  Neighbor Number: 2 / [-9]
repc_3_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 3 / [-8]
repc_4_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a19d.7c80
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 4 / [-7]
repc_4_12cs, Gi0/2 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 001a.a19d.7c80
  Port Number: 002
  Port Priority: 040
  Neighbor Number: 5 / [-6]

<output truncated>
```

This example shows output from the **show rep topology segment archive** command:

```
Switch# show rep topology segment 1 archive
REP Segment 1
BridgeName      PortName      Edge Role
-----
sw1_multseg_3750 Gi1/1/1      Pri  Open
sw3_multseg_3400 Gi1/13       Open
sw3_multseg_3400 Gi1/14       Open
sw4_multseg_3400 Gi1/13       Open
sw4_multseg_3400 Gi1/14       Open
sw5_multseg_3400 Gi1/13       Open
sw5_multseg_3400 Gi1/14       Open
sw2_multseg_3750 Gi1/1/2      Alt
sw2_multseg_3750 Gi1/1/1      Open
sw1_multseg_3750 Gi1/1/2      Sec  Open
```

#### Related Commands

Command	Description
<a href="#">rep segment</a>	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.

# show sdm prefer

To display information about the Switch Database Management (SDM) templates, use the **show sdm prefer** command in privileged EXEC mode.

```
show sdm prefer [default | lanbase-routing | dual-ipv4-and-ipv6 {default | routing} | qos |
routing]
[ | {begin | exclude | include} expression]
```

Syntax Description		
<b>default</b>	(Optional) Displays the template that balances system resources among features.	
<b>lanbase-routing</b>	(Optional) Displays the template that maximized system resources for static routes on SVIs.	
<b>dual-ipv4-and-ipv6</b> <b>{default   routing}</b>	(Optional) Displays the dual templates that support both IPv4 and IPv6. <ul style="list-style-type: none"> <li><b>default</b>—Displays the default dual template configuration.</li> <li><b>routing</b>—Displays the routing dual template configuration.</li> </ul>	
<b>qos</b>	(Optional) Displays the template that maximizes system resources for quality of service (QoS) access control entries (ACEs).	
<b>routing</b>	(Optional) Displays the template that maximizes system resources for IPv4 routing.	
<b>  begin</b>	(Optional) Begins with the line that matches the <i>expression</i> .	
<b>  exclude</b>	(Optional) Excludes lines that match the <i>expression</i> .	
<b>  include</b>	(Optional) Includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

<b>Command Modes</b>	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.
	12.2(52)SE	The <b>routing</b> and <b>dual-ipv4-and-ipv6 routing</b> keywords were added.
	15.0(2)SE	The <b>lanbase-routing</b> keyword was added.

**Usage Guidelines**

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

The numbers displayed for each 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* do not appear, but the lines that contain *Output* appear.

**Examples**

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:          12K
  number of IPv4 IGMP groups + multicast routes: 1K
  number of IPv4 unicast routes:            0
  number of IPv4 policy based routing aces:  0
  number of IPv4/MAC qos aces:              0.75K
  number of IPv4/MAC security aces:         1K
```

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

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

  number of unicast mac addresses:          8K
  number of IPv4 IGMP groups:               0.25K
  number of IPv4/MAC qos aces:              0.625k
  number of IPv4/MAC security aces:         0.125k
```

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

```
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:          2K
  number of IPv4 IGMP groups + multicast routes: 1K
  number of IPv4 unicast routes:            4K
    number of directly-connected IPv4 hosts: 2K
    number of indirect IPv4 routes:         2K
  number of IPv4 policy based routing aces:  0.5K
  number of IPv4/MAC qos aces:              0.625k
  number of IPv4/MAC security aces:         0.375k
```

This is an example of output from the **show sdm prefer dual-ip4-and-ipv6 routing** command:

```
Switch# show sdm prefer dual-ipv4-and-ipv6 routing
"dual-ipv4-and-ipv6 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:          1K
  number of IPv4 IGMP groups + multicast routes: 0.5K
  number of IPv4 unicast routes:            2K
    number of directly-connected IPv4 hosts: 1K
    number of indirect IPv4 routes:         1K
  number of IPv6 multicast groups:          0.625k
  number of directly-connected IPv6 addresses: 1K
  number of indirect IPv6 unicast routes:    0.375k
  number of IPv4 policy based routing aces:  0.125k
  number of IPv4/MAC qos aces:              0.375k
  number of IPv4/MAC security aces:         0.125k
  number of IPv6 policy based routing aces:  0.125k
```

```
number of IPv6 qos aces:          0.125k
number of IPv6 security aces:     0.125k
```

**Related Commands**

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

# show setup express

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

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

Syntax Description	<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.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

```
Switch# show setup express
express setup mode is active
```

Related Commands	Command	Description
	<a href="#">setup express</a>	Enables Express Setup mode.

# show spanning-tree

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

```
show spanning-tree [bridge-group | active [detail] | backbonefast | blockedports | bridge | detail
[active] | inconsistentports | interface interface-id | mst | pathcost method | root | summary
[totals] | uplinkfast | vlan vlan-id] [ | {begin | exclude | include} expression]
```

```
show spanning-tree bridge-group [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary] [ | {begin | exclude | include}
expression]
```

```
show spanning-tree vlan vlan-id [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary] [ | {begin | exclude | include}
expression]
```

```
show spanning-tree {vlan vlan-id | bridge-group} bridge [address | detail | forward-time |
hello-time | id | max-age | priority [system-id] | protocol] [ | {begin | exclude | include}
expression]
```

```
show spanning-tree {vlan vlan-id | bridge-group} root [address | cost | detail | forward-time |
hello-time | id | max-age | port | priority [system-id] [ | {begin | exclude | include}
expression]
```

```
show spanning-tree interface interface-id [active [detail] | cost | detail [active] | inconsistency |
portfast | priority | rootcost | state] [ | {begin | exclude | include} expression]
```

```
show spanning-tree mst [configuration [digest]] | [instance-id [detail | interface interface-id
[detail]] [ | {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 (available only in privileged EXEC mode).
<b>backbonefast</b>	(Optional) Display spanning-tree BackboneFast status.
<b>blockedports</b>	(Optional) Display blocked port information (available only 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 (optional keywords available only in privileged EXEC mode).
<b>detail</b> [ <b>active</b> ]	(Optional) Display a detailed summary of interface information ( <b>active</b> keyword available only in privileged EXEC mode).
<b>inconsistentports</b>	(Optional) Display inconsistent port information (available only 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 except <b>portfast</b> and <b>state</b> available only in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 6.

<b>mst</b> [ <b>configuration</b> [ <b>digest</b> ]] [ <i>instance-id</i> [ <b>detail</b>   <b>interface</b> <i>interface-id</i> [ <b>detail</b> ]]]	<p>(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode).</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>digest</b>—(Optional) Display the MD5 digest included in the current MST configuration identifier (MSTCI). Two separate digests, one for standard and one for prestandard switches, appear (available only in privileged EXEC mode).</li> </ul> <p>The terminology was updated for the implementation of the IEEE standard, and the <i>txholdcount</i> field was added.</p> <p>The new master role appears for boundary ports.</p> <p>The word <i>pre-standard</i> or <i>Pre-STD</i> appears when an IEEE standard bridge sends prestandard BPDUs on a port.</p> <p>The word <i>pre-standard (config)</i> or <i>Pre-STD-Cf</i> appears when a port has been configured to transmit prestandard BPDUs and no prestandard BPDU has been received on that port.</p> <p>The word <i>pre-standard (rcvd)</i> or <i>Pre-STD-Rx</i> appears when a prestandard BPDU has been received on a port that has not been configured to transmit prestandard BPDUs.</p> <p>A <i>dispute</i> flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated.</p> <ul style="list-style-type: none"> <li>• <i>instance-id</i>—You can specify a single instance ID, a range of IDs separated by a hyphen, or a series of IDs separated by a comma. The range is 1 to 4094. The display shows the number of currently configured instances.</li> <li>• <b>interface</b> <i>interface-id</i>—(Optional) Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 6.</li> <li>• <b>detail</b>—(Optional) Display detailed information for the instance or interface.</li> </ul>
<b>pathcost method</b>	(Optional) Display the default path cost method (available only 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 keywords available only 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. The words <i>IEEE Standard</i> identify the MST version running on a switch.
<b>uplinkfast</b>	(Optional) Display spanning-tree UplinkFast status.
<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 (some keywords available only in privileged EXEC mode). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.



<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** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was 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* do not appear, but the lines that contain *Output* appear.

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

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0001.42e2.cdd0
             Cost        3038
             Port        24 (GigabitEthernet1/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

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

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi1/1          Root FWD 3019      128.24  P2p
<output truncated>
```

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

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 1 (GigabitEthernet1/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times: hold 1, topology change 35, notification 2
         hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled
```

## show spanning-tree

```

Port 1 (GigabitEthernet1/1) of VLAN0001 is forwarding
  Port path cost 3019, Port priority 128, Port Identifier 128.24.
  Designated root has priority 32768, address 0001.42e2.cdd0
  Designated bridge has priority 32768, address 00d0.bbf5.c680
  Designated port id is 128.25, designated path cost 19
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 0, received 72364
<output truncated>

```

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

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

Vlan	Role	Sts	Cost	Prio.Nbr	Type
VLAN0001	Root	FWD	3019	128.24	P2p

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

```

Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is enabled
BackboneFast is enabled
Pathcost method used is short

```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	1	0	0	11	12
VLAN0002	3	0	0	1	4
VLAN0004	3	0	0	1	4
VLAN0006	3	0	0	1	4
VLAN0031	3	0	0	1	4
VLAN0032	3	0	0	1	4
<output truncated>					
37 vlans	109	0	0	47	156

Station update rate set to 150 packets/sec.

```
UplinkFast statistics
```

```

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

```

```
BackboneFast statistics
```

```

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

```

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

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

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

```
Switch# show spanning-tree mst interface gigabitEthernet1/1
GigabitEthernet1/1 of MST00 is root forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (STP) bpdu guard : disable (default)
Bpdus sent 5, received 74

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

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

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

Interface role state cost prio type
-----
GigabitEthernet1/1 root FWD 200000 128 P2P bound(STP)
GigabitEthernet1/2 desg FWD 200000 128 P2P bound(STP)
Port-channel1 desg FWD 200000 128 P2P bound(STP)
```

## Related Commands

Command	Description
<a href="#">clear spanning-tree counters</a>	Clears the spanning-tree counters.
<a href="#">clear spanning-tree detected-protocols</a>	Restarts the protocol migration process.
<a href="#">spanning-tree backbonefast</a>	Enables the BackboneFast feature.
<a href="#">spanning-tree bpdupfilter</a>	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
<a href="#">spanning-tree bpduguard</a>	Puts an interface 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 link-type</a>	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.

Command	Description
<b>spanning-tree loopguard default</b>	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
<b>spanning-tree mst configuration</b>	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
<b>spanning-tree mst cost</b>	Sets the path cost for MST calculations.
<b>spanning-tree mst forward-time</b>	Sets the forward-delay time for all MST instances.
<b>spanning-tree mst hello-time</b>	Sets the interval between hello BPDUs sent by root switch configuration messages.
<b>spanning-tree mst max-age</b>	Sets the interval between messages that the spanning tree receives from the root switch.
<b>spanning-tree mst max-hops</b>	Sets the number of hops in an MST region before the BPDU is discarded and the information held for an interface is aged.
<b>spanning-tree mst port-priority</b>	Configures an interface priority.
<b>spanning-tree mst priority</b>	Configures the switch priority for the specified spanning-tree instance.
<b>spanning-tree mst root</b>	Configures the MST root switch priority and timers based on the network diameter.
<b>spanning-tree port-priority</b>	Configures an interface priority.
<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an interface and all its associated VLANs.
<b>spanning-tree uplinkfast</b>	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
<b>spanning-tree vlan</b>	Configures spanning tree on a per-VLAN basis.

# show storm-control

Use the **show storm-control** 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, 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	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

Usage Guidelines	<p>When you enter an <i>interface-id</i>, the storm control thresholds appear for the specified interface.</p> <p>If you do not enter an <i>interface-id</i>, settings appear for one traffic type for all ports on the switch.</p> <p>If you do not enter a traffic type, settings appear for broadcast storm control.</p> <p>Expressions are case sensitive. For example, if you enter   <b>exclude output</b>, the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.</p>
------------------	--

Examples	<p>This is an example of a partial output from the <b>show storm-control</b> command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.</p>
----------	--

```
Switch> show storm-control
Interface  Filter State  Upper      Lower      Current
-----
Gi1/1     Forwarding    20 pps     10 pps     5 pps
Gi1/2     Forwarding    50.00%     40.00%     0.00%
<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 appear.

```
Switch> show storm-control gigabitethernet 1/1
Interface   Filter State   Upper   Lower   Current
-----
Gi1/1      Forwarding    20 pps  10 pps  5 pps
```

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>
Upper	Displays the rising suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Lower	Displays the falling suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Current	Displays the bandwidth usage 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
<a href="#">storm-control</a>	Sets the broadcast, multicast, or unicast storm control levels for the switch.

# 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
	12.2(44)EX	This command was introduced.

Usage Guidelines	If you have used the <b>system mtu</b> or <b>system mtu jumbo</b> 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 ports operating at 10/100 Mb/s; the system jumbo MTU refers to Gigabit ports; the system routing MTU refers to routed ports.
	Expressions are case sensitive. For example, if you enter   <b>exclude output</b> , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.

Examples	This is an example of output from the <b>show system mtu</b> command:
----------	---

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1550 bytes
Routing MTU size is 1500 bytes.
```

Related Commands	Command	Description
	<a href="#">system mtu</a>	Sets the MTU size for the Fast Ethernet, Gigabit Ethernet, or routed ports.

# show udld

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

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

## Syntax Description

<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

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.

## Usage Guidelines

If you do not enter an *interface-id*, administrative and operational UDLD status for all interfaces appear. Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples


This is an example of output from the **show udld interface-id** 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 udld gigabitethernet1/1
Interface gi1/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
  Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi1/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi1/2
    Message interval: 5
    CDP Device name: Switch-A
```



**Table 2-19**      *show uddld Field Descriptions*

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The 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 appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

 show uddl

Related Commands	Command	Description
	<a href="#">uddl</a>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	<a href="#">uddl port</a>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>uddl</b> global configuration command.
	<a href="#">uddl reset</a>	Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again.

# show version

Use the **show version** 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	EXEC
---------------	------

Command History	Release	Modification
	12.2(44)EX	This command was introduced.

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

Examples	This is an example of output from the <b>show version</b> command:
----------	--



## Note

Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

```
switch# show version
Cisco IOS Software, IES Software (IES-LANBASE-M), Version 12.2(44)EX, RELEASE SOFTWARE
(fc2) Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 19-May-08 12:47 by weiliu
Image text-base: 0x00003000, data-base: 0x01400000

ROM: Bootstrap program is IE 3000 boot loader
BOOTLDR: IES Boot Loader (IES-HBOOT-M), Version 12.2 [mchou-v122ldr0328 102]

Switch uptime is 2 days, 1 hour, 36 minutes System returned to ROM by power-on System
image file is ''flash:/ies-lanbase-mz.122-44.EX/ies-lanbase-mz.122-44.EX.bin''

cisco IE-3000-4TC (PowerPC405) processor with 126976K/4088K bytes of memory.
Processor board ID FHK1152UZRW
Last reset from power-on
1 Virtual Ethernet interface
20 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
```

# show version

```

Base ethernet MAC Address      : 00:1E:13:00:2D:00
Motherboard assembly number    : 73-10855-07
Motherboard serial number      : FOC115040S9
Motherboard revision number    : 04
Model number                   : IE-3000-4TC
System serial number           : FHK1152UZRW
Top Assembly Part Number       : 800-28491-01
Hardware Board Revision Number : 0x02
CIP Serial Number              : 0x43313135
SKU Brand Name                 : Cisco

Switch Ports Model          SW Version  SW Image
-----
*    1 22    IE-3000-4TC    12.2(44)EX    IES-LANBASE-M

Configuration register is 0xF

```

# show vlan

Use the **show vlan** 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** | **mtu** | **name** *vlan-name* | **private-vlan** [**type**] | **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 a 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>mtu</b>	(Optional) Display a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.	
<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>private-vlan</b>	(Optional) Display information about configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and ports belonging to the private VLAN. This keyword is only supported if your switch is running the IP services image.	
<b>type</b>	(Optional) Display only private VLAN ID and type.	
<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** keyword is not supported.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(44)EX	This command was introduced.
	12.2(52)SE	The <b>dot1q tag native</b> , <b>internal usage</b> , and <b>private-vlan</b> keywords were added.

**Usage Guidelines**

In the **show vlan mtu** command output, the MTU\_Mismatch column shows whether all the ports in the VLAN have the same MTU. When *yes* appears in this column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI\_MTU column. If the MTU-Mismatch column displays *yes*, the names of the port with the MinMTU and the port with the MaxMTU appear.

If you try to associate a private VLAN secondary VLAN with a primary VLAN before you define the secondary VLAN, the secondary VLAN is not included in the **show vlan private-vlan** command output.

In the **show vlan private-vlan type** command output, a type displayed as *normal* means a VLAN that has a private VLAN association but is not part of the private VLAN. For example, if you define and associate two VLANs as primary and secondary VLANs and then delete the secondary VLAN configuration without removing the association from the primary VLAN, the VLAN that was the secondary VLAN is shown as *normal* in the display. In the **show vlan private-vlan** output, the primary and secondary VLAN pair is shown as *non-operational*.

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

**Examples**

This is an example of output from the **show vlan** command. [Table 2-20](#) describes the fields in the display.

```
Switch> show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa1/1, Fa1/2, Fa1/3, Fa1/4 Fa2/1, Fa2/2, Fa2/3, Fa2/4 Fa2/5, Fa2/6, Fa2/7, Fa2/8 Fa3/1, Fa3/2, Fa3/3, Fa3/4 Fa3/5, Fa3/6, Fa3/7, Fa3/8 Gi1/1, Gi1/2
2	Tes	active	Fa1/3, Fa2/5, Fa2/6
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```
Remote SPAN VLANs
```

Primary	Secondary	Type	Ports
20	25	isolated	Fa1/13, Fa1/20, Fa1/22, Gi1/1,
20	30	community	Fa1/1, Fa1/20, Fa1/21, Gi1/1,

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3 Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9

```

Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15
Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20, Fa0/21
Fa0/24, Gi0/1, Gi0/2

<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
-----

Primary Secondary Type Ports
-----
20    25    isolated Fa0/13, Fa0/20, Fa0/22, Gi0/1,
20    30    community Fa0/13, Fa0/20, Fa0/21, Gi0/1
20    35    community Fa0/13, Fa0/20, Fa0/23, Fa0/33, Gi0/1

<output truncated>

```

**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.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.

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

Field	Description
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.
Primary/Secondary/Type/Ports	Includes any private VLANs that have been configured, including the primary VLAN ID, the secondary VLAN ID, the type of secondary VLAN (community or isolated), and the ports that belong to it.

This is an example of output from the **show vlan dot1q tag native** command:

```
Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

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

```
Switch> show vlan private-vlan
Primary Secondary Type          Ports
-----
10      501      isolated      Gi1/3
10      502      community     Fa1/11
10      503      non-operational3  -
20      25      isolated      Fa1/1, Fa1/20, Fa1/22, Gi1/1, Fa1/13,
                        Fa1/3, Fa1/2, Fa1/4,
20      30      community     Fa1/13, Fa1/20, Fa1/21, Gi1/1, Fa1/10,
20      55      non-operational
```

This is an example of output from the **show vlan private-vlan type** command:

```
Switch> show vlan private-vlan type
Vlan Type
-----
10  primary
501 isolated
502 community
503 normal
```

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     Fa1/3, Fa2/5, Fa2/6

2    VLAN0200                active     Fa1/3, Fa2/5, Fa2/6
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. 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 FastEthernet1/23
1026 FastEthernet1/24

```

Related Commands	Command	Description
	<b>private-vlan</b>	Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs.
	<b>switchport mode</b>	Configures the VLAN membership mode of a port.
	<b>vlan</b>	Enables VLAN configuration mode where you can configure VLANs 1 to 4094.

# show vlan access-map

Use the **show vlan access-map** privileged EXEC command to display information about a particular VLAN access map or for all VLAN access maps.

**show vlan access-map** [*mapname*] [ | { **begin** | **exclude** | **include** } *expression* ]



## Note

This command is available only when the switch is running the IP Services image.

## 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
12.2(52)SE	This command was introduced.

## Usage Guidelines

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

## Examples

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

```
Switch# show vlan access-map
Vlan access-map "SecWiz" 10
  Match clauses:
    ip address: SecWiz_Gi0_3_in_ip
    ip address: SecWiz_Fa10_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*]



## Note

This command is available only when the switch is running the IP Services image.

## Syntax 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
12.2(52)SE	This command was introduced.

## Usage Guidelines

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

## Examples

This is an example of output from the **show 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 for 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** 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	<b>statistics</b>	(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	EXEC
---------------	------

Command History	<b>Release</b>	<b>Modification</b>
	12.2(44)EX	This command was introduced.

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

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

```
Switch> show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:
```

```
Reconfirmation status
-----
VMPS Action:          other
```

This is an example of output from the **show vmps statistics** command. [Table 2-21](#) describes each field in the display.

```
Switch> show vmps statistics
VMPS Client Statistics
-----
VQP  Queries:                0
VQP  Responses:              0
VMPS  Changes:                0
VQP  Shutdowns:              0
VQP  Denied:                  0
VQP  Wrong Domain:           0
```

```
VQP Wrong Version:          0
VQP Insufficient Resource: 0
```

**Table 2-21** *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>clear vmmps statistics</b>	Clears the statistics maintained by the VQP client.
<b>vmmps reconfirm (privileged EXEC)</b>	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** EXEC command to display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters.

```
show vtp {counters | devices [conflicts] | interface [interface-id] | password | status} [ | {begin |
exclude | include} expression]
```

## Syntax Description

<b>counters</b>	Display the VTP statistics for the switch.
<b>password</b>	Display the configured VTP password.
<b>devices</b>	Display information about all VTP version 3 devices in the domain. This keyword applies only if the switch is not running VTP version 3.
<b>conflicts</b>	(Optional) Display information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the switch is in VTP transparent or VPT off mode.
<b>interface</b> [interface-id]	Display VTP status and configuration for all interfaces or the specified interface. The <i>interface-id</i> can be a physical interface or a port channel.
<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

EXEC

## Command History

Release	Modification
12.2(44)EX	This command was introduced.
12.2(52)SE	The <b>devices</b> and <b>interface</b> keywords were added for VTP version 3.

## Usage Guidelines

When you enter the **show vtp password** command when the switch is running VTP version 3, the display follows these rules:

- If the **password** *password* global configuration command did not specify the **hidden** keyword and encryption is not enabled on the switch, the password appears in clear text.
- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the switch, the encrypted password appears.
- If the **password** *password* command included the **hidden** keyword, the hexadecimal secret key is displayed.

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

**Examples**

This is an example of output from the **show vtp devices** command. A *Yes* in the *Conflict* column means that the responding server is in conflict with the local server for the feature; that is, when two switches in the same domain do not have the same primary server for a database.

```
Switch# show vtp devices
```

```
Retrieving information from the VTP domain. Waiting for 5 seconds.
```

```
VTP Database Conf switch ID      Primary Server Revision  System Name
      list
-----
VLAN      Yes  00b0.8e50.d000  000c.0412.6300 12354      main.cisco.com
MST       No   00b0.8e50.d000  0004.AB45.6000 24         main.cisco.com
VLAN      Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

This is an example of output from the **show vtp counters** command. [Table 2-22](#) describes the fields in the display.

```
Switch> show vtp counters
```

```
VTP statistics:
```

```
Summary advertisements received      : 0
Subset advertisements received       : 0
Request advertisements received      : 0
Summary advertisements transmitted   : 6970
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
-----
Fal/7      0              0              0
Fal/8      0              0              0
Gi1/1      0              0              0
Gi1/2      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.

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

Field	Description
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>
Number of V1 summary errors	<p>Number of Version 1 errors.</p> <p>Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP Version 1 frame. These errors mean that at least one neighboring switch is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.</p>
Join Transmitted	Number of VTP pruning messages 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 for a switch running VTP version 2. [Table 2-23](#) describes the fields 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.
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 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.

This is an example of output from the **show vtp status** command for a switch running VTP version 3. .

```
Switch> show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 3
VTP Domain Name         : Cisco
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 0021.1bcd.c700

Feature VLAN:
-----
VTP Operating Mode      : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision  : 0
Primary ID              : 0000.0000.0000
Primary Description     :
MD5 digest              : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                        : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
-----
VTP Operating Mode      : Client
Configuration Revision  : 0
Primary ID              : 0000.0000.0000
Primary Description     :
MD5 digest              : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                        : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
-----
VTP Operating Mode      : Transparent
```

## Related Commands

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