rmon collection stats

Use the **rmon collection stats** interface configuration command on the switch stack or on a standalone switch to collect Ethernet group statistics, which include 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*]

Syntax Description

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

Defaults

The RMON statistics collection is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(40)EX2	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 gigabitethernet2/0/1
Switch(config-if)# rmon collection stats 2 owner root
```

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

Related Commands

Command	Description
show rmon statistics	Displays RMON statistics. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > System Management Commands > RMON Commands.**

sdm prefer

Use the **sdm prefer** global configuration command on the switch stack or on a standalone switch to configure the template used in Switch Database Management (SDM) resource allocation. You can use a template to allocate system resources to best support the features being used in your application. Use a template to provide maximum system usage for unicast routing or for VLAN configuration or to select the dual IPv4 and IPv6 template to support IPv6 forwarding. Use the **no** form of this command to return to the default template.

sdm prefer {**access** | **default** | **dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} | **routing** | **vlan**}

no sdm prefer

Syntax Description

access	Provide maximum system usage for access control lists (ACLs). Use this template if you have a large number of ACLs.
default	Give balance to all functions.
dual-ipv4-and-ipv6 {**default** | **routing** | **vlan**}	Select a template that supports both IPv4 and IPv6 routing. • **default**—Provide balance to IPv4 and IPv6 Layer 2 and Layer 3 functionality. • **routing**—Provide maximum system usage for IPv4 and IPv6 routing, including IPv4 policy-based routing. • **vlan**—Provide maximum system usage for IPv4 and IPv6 VLANs.
routing	Provide maximum system usage for unicast routing. You would typically use this template for a router in the middle of a network.
vlan	Provide maximum system usage for VLANs. This template maximizes system resources for use as a Layer 2 switch with no routing.

Defaults

The default template provides a balance to all features.

Command Modes

Global configuration

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

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.

Follow these guidelines for the Catalyst Switch Module 3110:

- All stack members use the same SDM desktop template that is stored on the stack master. When a new switch member is added to a stack, the stored SDM configuration overrides the template configured on an individual switch.
- The IPv6 packets are routed in hardware across the stack, as long as the packet does not have exceptions (IPv6Options) and the switches have not run out of hardware resources.
- If a stack member cannot support the template that is running on the master switch, the switch goes into SDM mismatch mode, the master switch does not attempt to change the SDM template, and the switch cannot be a functioning member of the stack.

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

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

The access template maximizes system resources for access control lists (ACLs) as required to accommodate a large number of ACLs.

The default templates balances the use of system resources.

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

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

Do not use the ipv4-and-ipv6 templates if you do not plan to enable IPv6 routing on the switch. Entering the **sdm prefer ipv4-and-ipv6** {**default** | **routing** | **vlan**} global configuration command divides resources between IPv4 and IPv6, limiting those allocated to IPv4 forwarding.

Table 2-15 lists the approximate number of each resource that is supported in each of the IPv4-only templates for a desktop switch. The values in the template are based on 8 routed interfaces and 1024 VLANs and represent the 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.

Table 2-15 Approximate Number of Feature Resources Allowed by IPv4 Templates

Resource	Access	Default	Routing	VLAN
Unicast MAC addresses	4 K	6 K	3 K	12 K
Internet Group Management Protocol (IGMP) groups and multicast routes	1 K	1 K	1 K	1 K
Unicast routes	6 K	8 K	11 K	0
• Directly connected hosts	4 K	6 K	3 K	0
• Indirect routes	2 K	2 K	8 K	0
Policy-based routing access control entries (ACEs)	0.5 K	0	0.5 K	0
Quality of service (QoS) classification ACEs	0.5 K	0.5 K	0.5 K	0.5 K
Security ACEs	2 K	1 K	1 K	1 K
VLANs	1 K	1 K	1 K	1 K

Table 2-16 lists the approximate number of each resource supported in each of the dual IPv4-and IPv6 templates for a desktop switch.

Table 2-16 Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates

Resource	Default	Routing	VLAN
Unicast MAC addresses	2 K	1.5 K	8 K
IPv4 IGMP groups and multicast routes	1 K	1 K	1 K for IGMP groups 0 for multicast routes
Total IPv4 unicast routes:	3 K	2.75 K	0
• Directly connected IPv4 hosts	2 K	1.5 K	0
• Indirect IPv4 routes	1 K	1.25 K	0
IPv6 multicast groups	1 K	1 K	1 K
Directly connected IPv6 addresses	2 K	1.5 K	0
Indirect IPv6 unicast routes	1 K	1.25 K	0
IPv4 policy-based routing ACEs	0	0.25 K	0
IPv4 or MAC QoS ACEs (total)	0.5 K	0.5 K	0.5 K
IPv4 or MAC security ACEs (total)	1 K	0.5 K	1 K
IPv6 security ACEs	1 K	1 K	0.5 K

Examples

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

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

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

```
Switch(config)# sdm prefer routing
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 change a switch template to the default template.

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

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

Related Commands

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

service password-recovery

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

service password-recovery

no service password-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

The password-recovery mechanism is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

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

If the password-recovery mechanism is disabled, this message appears:

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

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

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

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

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

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

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

Examples

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

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

Related Commands

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

service-policy

Use the **service-policy** interface configuration command on the switch stack or on a standalone switch to apply a policy map defined by the **policy-map** command to the input of a 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(40)EX2	This command was introduced.

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

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

```
Switch(config)# interface gigabitethernet2/0/2
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> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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#
Switch#
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input gigabitethernet3/0/1 - gigabitethernet3/0/2
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)# 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)# exit
Switch(config-pmap)# class-map cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap)# exit
Switch(config)# int vlan 10
Switch(config-if)#
Switch(config-if)# ser input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

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

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command.

session

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

session *stack-member-number*

Note This command is supported only on stacking-capable switches.

Syntax Description

stack-member-number	Specify the stack member number. The range is 1 to 9.

Defaults

No default is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to access stack member 6:

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

Related Commands

Command	Description
reload	Reloads the stack member and puts a configuration change into effect.
switch priority	Changes the stack member priority value.
switch renumber	Changes the stack member number.
show switch	Displays information about the switch stack and its stack members.

set

Use the **set** policy-map class configuration command on the switch stack or on a standalone switch to classify IP traffic by setting a Differentiated Services Code Point (DSCP) or 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

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

Defaults

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

If you have used the **set ip dscp p**olicy-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
class	Defines a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.
trust	Defines a trust state for traffic classified through the **class** policy-map configuration command or the **class-map** global configuration command.

setup

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

setup

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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

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

GigabitEthernet6/0/1         unassigned      YES unset  up                    up

GigabitEthernet6/0/2         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$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet6/0/1
no ip address
!
interface GigabitEthernet6/0/2
no ip address
!

end
```

```
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

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

[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

Related Commands

Command	Description
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command.
show version	Displays version information for the hardware and firmware.

setup express

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

setup express

no setup express

Syntax Description

This command has no arguments or keywords.

Defaults

Express Setup is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

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

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

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

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

Examples

This example shows how to enable Express Setup mode:

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

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

- On an unconfigured switch, the LEDs above the Mode 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 Mode button down for a total of 10 seconds, the configuration is deleted, and the switch reboots.

This example shows how to disable Express Setup mode:

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

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

Related Commands

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

show access-lists

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

show access-lists [*name* | *number* | **hardware counters** | **ipc**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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

Examples

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

```
Switch# show access-lists
Standard IP access list 1
    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
access-list	Configures a standard or extended numbered access list on the switch. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands.**
ip access list	Configures a named IP access list on the switch. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands.**
mac access-list extended	Configures a named or numbered MAC access list on the switch.

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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

Examples

These are examples of output from the **show 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
archive download-sw	Downloads a new image from a TFTP server to the switch.

show arp access-list

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

show arp access-list [*acl-name*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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
arp access-list	Defines an ARP ACL.
deny (ARP access-list configuration)	Denies an ARP packet based on matches against the Dynamic Host Configuration Protocol (DHCP) bindings.
ip arp inspection filter vlan	Permits ARP requests and responses from a host configured with a static IP address.
permit (ARP access-list configuration)	Permits an ARP packet based on matches against the DHCP bindings.

show auto qos

Use the **show auto qos** user 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

interface [*interface-id*]	(Optional) Display auto-QoS information for the specified port or for all ports. Valid interfaces include physical ports.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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
GigabitEthernet2/0/4
auto qos voip cisco-softphone

GigabitEthernet2/0/5
auto qos voip cisco-phone

GigabitEthernet2/0/6
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 2/0/5
GigabitEthernet2/0/5
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 GigabitEthernet2/0/4
 switchport mode access
 switchport port-security maximum 400
 service-policy input AutoQoS-Police-SoftPhone
 speed 100
 duplex half
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 auto qos voip cisco-softphone
!
interface GigabitEthernet2/0/5
 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 GigabitEthernet2/0/6
 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 GigabitEthernet4/0/1
 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 gigabitethernet1/0/2
GigabitEthernet1/0/2
auto qos voip cisco-phone
```

These are examples 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
```

These are examples of output from the **show auto qos interface** *interface-id* command when auto-QoS is disabled on an interface:

```
Switch> show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled
```

Related Commands

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

show boot

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show boot** command for all stack members.

```
Switch# show boot
BOOT path-list      : flash:cbs31x0-universal-mz
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : yes
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   :
-------------------
Switch 2
-------------------
BOOT path-list      : flash:cbs31x0-universal-mz
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : yes
HELPER path-list    :

Auto upgrade        : no
Auto upgrade path   :
-------------------
<output truncated>
```

Table 2-17 describes each field in the display.

Table 2-17 show boot Field Descriptions

Field	Description
BOOT path-list	Displays a semicolon separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
Config file	Displays the filename that 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 is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to no or 0, the boot loader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the boot loader mode.
Helper path-list	Displays a semicolon separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
Auto upgrade	On the Catalyst Switch Module 3110, displays whether the switch stack is set to automatically copy its software version to an incompatible switch so that it can join the stack. A switch in version-mismatch (VM) mode is a switch that has a different stack protocol version than the version on the switch stack. Switches in VM mode cannot join the switch stack. If the switch stack has an image that can be copied to a switch in VM mode, and if the **boot auto-copy-sw** feature is enabled, the switch stack automatically copies the image from another stack member to the switch in VM mode. The switch then exits VM mode, reboots, and joins the switch stack.
NVRAM/Config file buffer size	On the Catalyst Switch Module 3012, 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
boot auto-copy-sw	Enables the automatic upgrade (auto-upgrade) process to automatically upgrade a switch in version-mismatch (VM) mode. This command is supported only on the Catalyst Switch Module 3110.
boot auto-download-sw	Specifies the software image to use in the auto-upgrade process. This command is supported only on the Catalyst Switch Module 3110.
boot config-file	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
boot enable-break	Enables interrupting the automatic boot process.
boot manual	Enables manually booting the switch during the next boot cycle.
boot private-config-file	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration.
boot system	Specifies the Cisco IOS image to load during the next boot cycle.

show cable-diagnostics tdr

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports. For more information about TDR, see the software configuration guide for this release.

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

Examples

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

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
TDR test last run on: March 01 00:04:08
Interface  Speed  Local pair  Pair length        Remote pair   Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi1/0/2    1000M  Pair A      1    +/- 1 meters   Pair A        Normal
                  Pair B      1    +/- 1 meters   Pair B        Normal
                  Pair C      1    +/- 1 meters   Pair C        Normal
                  Pair D      1    +/- 1 meters   Pair D        Normal
```

Table 2-18 lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

Table 2-18 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.

Table 2-18 Fields Descriptions for the show cable-diagnostics tdr Command Output (continued)

Field	Description
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s. • The cable is open. • The cable has a short.
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can 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: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted. • ImpedanceMis—The impedance is mismatched. • Short/Impedance Mismatched—The impedance mismatched or the cable is short. • InProgress—The diagnostic test is in progress

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

```
Switch# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 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 gigabitethernet1/0/2
% TDR test was never issued on Gi1/0/2
```

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

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

Related Commands

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

show class-map

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

Related Commands

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

<output truncated>

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

<output truncated>

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

<output truncated>
```

Related Commands

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

show controllers ethernet-controller

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

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

Syntax Description

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

Command Modes

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

Command History

Release	Modification
12.2(40)EX2	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.

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

Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface. Table 2-19 describes the *Transmit* fields, and Table 2-20 describes the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitethernet6/0/1
Transmit GigabitEthernet6/0/1            Receive
         0 Bytes                              0 Bytes
         0 Unicast frames                     0 Unicast frames
         0 Multicast frames                   0 Multicast frames
         0 Broadcast frames                   0 Broadcast frames
         0 Too old frames                     0 Unicast bytes
         0 Deferred frames                    0 Multicast bytes
         0 MTU exceeded frames                0 Broadcast bytes
         0 1 collision frames                 0 Alignment errors
         0 2 collision frames                 0 FCS errors
         0 3 collision frames                 0 Oversize frames
         0 4 collision frames                 0 Undersize frames
         0 5 collision frames                 0 Collision fragments
         0 6 collision frames
         0 7 collision frames                 0 Minimum size frames
         0 8 collision frames                 0 65 to 127 byte frames
         0 9 collision frames                 0 128 to 255 byte frames
         0 10 collision frames                0 256 to 511 byte frames
         0 11 collision frames                0 512 to 1023 byte frames
         0 12 collision frames                0 1024 to 1518 byte frames
         0 13 collision frames                0 Overrun frames
         0 14 collision frames                0 Pause frames
         0 15 collision frames                0 Symbol error frames
         0 Excessive collisions
         0 Late collisions                    0 Invalid frames, too large
         0 VLAN discard frames                0 Valid frames, too large
         0 Excess defer frames                0 Invalid frames, too small
         0 64 byte frames                     0 Valid frames, too small
         0 127 byte frames
         0 255 byte frames                    0 Too old frames
         0 511 byte frames                    0 Valid oversize frames
         0 1023 byte frames                   0 System FCS error frames
         0 1518 byte frames                   0 RxPortFifoFull drop frame
         0 Too large frames
         0 Good (1 coll) frames
```

Table 2-19 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 2-19 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[1] 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 2-20 Receive Field Descriptions

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

Table 2-20 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[2] 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 2-20 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 gigabitethernet1/0/2 phy
Control Register                      :  0001 0001 0100 0000
 Control STATUS                        :  0111 1001 0100 1001
 Phy ID 1                              :  0000 0001 0100 0001
 Phy ID 2                              :  0000 1100 0010 0100
 Auto-Negotiation Advertisement        :  0000 0011 1110 0001
 Auto-Negotiation Link Partner         :  0000 0000 0000 0000
 Auto-Negotiation Expansion Reg        :  0000 0000 0000 0100
 Next Page Transmit Register           :  0010 0000 0000 0001
 Link Partner Next page Registe        :  0000 0000 0000 0000
 1000BASE-T Control Register           :  0000 1111 0000 0000
 1000BASE-T Status Register            :  0100 0000 0000 0000
 Extended Status Register              :  0011 0000 0000 0000
 PHY Specific Control Register         :  0000 0000 0111 1000
 PHY Specific Status Register          :  1000 0001 0100 0000
 Interrupt Enable                      :  0000 0000 0000 0000
 Interrupt Status                      :  0000 0000 0100 0000
 Extended PHY Specific Control         :  0000 1100 0110 1000
 Receive Error Counter                 :  0000 0000 0000 0000
 Reserved Register 1                   :  0000 0000 0000 0000
 Global Status                         :  0000 0000 0000 0000
 LED Control                           :  0100 0001 0000 0000
 Manual LED Override                   :  0000 1000 0010 1010
 Extended PHY Specific Control         :  0000 0000 0001 1010
 Disable Receiver 1                    :  0000 0000 0000 1011
 Disable Receiver 2                    :  1000 0000 0000 0100
 Extended PHY Specific Status          :  1000 0100 1000 0000
 Auto-MDIX                             :  On   [AdminState=1   Flags=0x00052248]
```

This is an example of output from the **show controllers ethernet-controller tengigabitethernet1/0/1 phy** command:

```
Switch# show controllers ethernet-controller tengigabitethernet1/0/1 phy
TenGigabitEthernet1/0/1 (gpn: 29, port-number: 1)
-----------------------------------------------------------
X2 Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
X2 MSA Version supported :0x1E
NVR Size in bytes :0x100
Number of bytes used :0x100
Basic Field Address :0xB
Customer Field Address :0x77
Vendor Field Address :0xA7
Extended Vendor Field Address :0x100
Reserved :0x0
Transceiver type :0x2 =X2
Optical connector type :0x1 =SC
```

```
Bit encoding:0x1 =NRZ
Normal BitRate in multiple of 1M b/s :0x2848
Protocol Type:0x1 =10GgE
Standards Compliance Codes :
10GbE Code Byte 0 :0x4 =10GBASE-ER
10GbE Code Byte 1 :0x0
SONET/SDH Code Byte 0:0x0
SONET/SDH Code Byte 1:0x0
SONET/SDH Code Byte 2:0x0
SONET/SDH Code Byte 3:0x0
10GFC Code Byte 0 :0x0
10GFC Code Byte 1 :0x0
10GFC Code Byte 2 :0x0
10GFC Code Byte 3 :0x0
Transmission range in10m :0xFA0
Fibre Type :
Fibre Type Byte 0 :0x20 =SM, Generic
Fibre Type Byte 1 :0x0 =Unspecified
<output truncated>
```

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

```
Switch# show controllers ethernet-controller port-asic configuration
========================================================================
Switch 1, PortASIC 0 Registers
------------------------------------------------------------------------
DeviceType                         : 000101BC
Reset                              : 00000000
PmadMicConfig                      : 00000001
PmadMicDiag                        : 00000003
SupervisorReceiveFifoSramInfo      : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo     : 000001D0 000001D0 40000000
GlobalStatus                       : 00000800
IndicationStatus                   : 00000000
IndicationStatusMask               : FFFFFFFF
InterruptStatus                    : 00000000
InterruptStatusMask                : 01FFE800
SupervisorDiag                     : 00000000
SupervisorFrameSizeLimit           : 000007C8
SupervisorBroadcast                : 000A0F01
GeneralIO                          : 000003F9 00000000 00000004
StackPcsInfo                       : FFFF1000 860329BD 5555FFFF FFFFFFFF
                                     FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo                       : 73001630 00000003 7F001644 00000003
                                     24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus                 : 18E418E0
stackControlStatusMask             : FFFFFFFF
TransmitBufferFreeListInfo         : 00000854 00000800 00000FF8 00000000
                                     0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo               : 00000016 00000016 40000000 00000000
                                     0000000C 0000000C 40000000 00000000
TransmitBufferInfo                 : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount          : 00000F7A
TransmitBufferCommonCountPeak      : 0000001E
TransmitBufferCommonCommonEmpty    : 000000FF
NetworkActivity                    : 00000000 00000000 00000000 02400000
DroppedStatistics                  : 00000000
FrameLengthDeltaSelect             : 00000001
SneakPortFifoInfo                  : 00000000
MacInfo                            : 0EC0801C 00000001 0EC0801B 00000001
                                     00C0001D 00000001 00C0001E 00000001

<output truncated>
```

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

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

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

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

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


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

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

<output truncated>
```

Related Commands

Command	Description
show controllers cpu-interface	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
show controllers tcam	Displays the state of registers for all hardware memory in the system and for hardware interface ASICs that are content addressable memory controllers.
show idprom	Displays the IDPROM information for the specified interface.

show controllers ethernet-controller fastethernet

Use the **show controllers ethernet-controller fastethernet** privileged EXEC command to display information about the Ethernet management port, including the port status and the per-interface send and receive statistics read from the hardware.

show controllers ethernet-controller fastethernet 0 [**phy** [**detail**] | **stack**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

phy [**detail**]	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the Ethernet management port on the switch when the command is entered on a switch. Display the status of the internal registers on the switch PHYs for all the Ethernet management ports in the switch stack when the command is entered on a stack master or member. Use the **detail** keyword to display details about the PHY internal registers. This display includes the operational state of the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface.
stack	(Optional) Display the speed, duplex mode, and link states of the Ethernet management ports in the switch stack when the command is entered on a stack master or member.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (only supported with the **fastethernet 0** keywords in user EXEC mode)

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

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

Examples

This is an example of output from the **show controllers ethernet-controller fastethernet 0** command. See Table 2-19 and Table 2-20 for descriptions of the *Transmit* and *Receive* fields.

```
Switch> show controller ethernet-controller fastethernet 0
     Transmit FastEthernet0                   Receive
         5925 Bytes                            33181 Bytes
            0 Unicast frames                      78 Unicast frames
           15 Multicast frames                   437 Multicast frames
            1 Broadcast frames                     0 Broadcast frames
            0 Too old frames                       0 Unicast bytes
            0 Deferred frames                      0 Multicast bytes
            0 MTU exceeded frames                  0 Broadcast bytes
            0 1 collision frames                   0 Alignment errors
            0 2 collision frames                   0 FCS errors
            0 3 collision frames                   0 Oversize frames
            0 4 collision frames                   0 Undersize frames
            0 5 collision frames                   0 Collision fragments
            0 6 collision frames
            0 7 collision frames                   0 Minimum size frames
            0 8 collision frames                   0 65 to 127 byte frames
            0 9 collision frames                   0 128 to 255 byte frames
            0 10 collision frames                  0 256 to 511 byte frames
            0 11 collision frames                  0 512 to 1023 byte frames
            0 12 collision frames                  0 1024 to 1518 byte frames
            0 13 collision frames                  0 Overrun frames
            0 14 collision frames                  0 Pause frames
            0 15 collision frames
            0 Excessive collisions                 0 Symbol error frames
            0 Late collisions                      0 Invalid frames, too large
            0 VLAN discard frames                  0 Valid frames, too large
            0 Excess defer frames                  0 Invalid frames, too small
            0 64 byte frames                       0 Valid frames, too small
            0 127 byte frames
            0 255 byte frames                      0 Too old frames
            0 511 byte frames                      0 Valid oversize frames
            0 1023 byte frames                     0 System FCS error frames
            0 1518 byte frames                     0 RxPortFifoFull drop frame
            0 Too large frames
            0 Good (1 coll) frames
            0 Good (>1 coll) frames
```

This is an example of output from the **show controllers ethernet-controller fastethernet 0 phy** command:

```
Switch# show controller ethernet-controller fastethernet 0 phy
FastEthernet0
------------------------------------------------------------
hw_if_index = 2 if_number = 2
PowerPC405 FastEthernet unit 0
PHY Hardware is Broadcom BCM5220 rev. 4 (id_register: 0x40, 0x61E4)

rx_intr: 0 tx_intr: 0 mac_err_isr: 0 phy_link_isr:0
Current station address 00d0.2bfd.d737, default address 00d0.2bfd.d737
MAL register dump:
malcr         0x00004082  0x100
malesr        0x00000000  0x101
malier        0x00000000  0x102
maltxcasr     0x80000000  0x104
maltxcarr     0x80000000  0x105
maltxeobisr   0x80000000  0x106
maltxdeir     0x00000000  0x107
malrxcasr     0x80000000  0x110
malrxcarr     0x80000000  0x111
```

```
malrxeobisr  0x80000000  0x112
malrxdeir    0x00000000  0x113
maltxctp0r   0x0F027880  0x120
malrxctp0r   0x0F0272C0  0x140
malrcbs0   0x00000060  0x160

<output truncated>
```

This is an example of output from the **show controllers ethernet-controller fastethernet 0 stack** command on a stack member:

```
Switch# show controller ethernet-controller fastethernet 0 stack
Switch   Interface-Name   Duplex   Speed   Link-State   Active-Link
-------------------------------------------------------------------
     3   Fa0              a-full   a-100           up
     3   Fa0-Physical     a-full   a-100           up         *
```

Related Commands

Command	Description
debug fastethernet	Enables debugging of the Ethernet management port.

show controllers tcam

Use the **show controllers tcam** privileged EXEC command to display the state of the registers for all hardware memory in the system and for all hardware interface ASICs that are content-addressable memory-controllers.

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
Switch# show controllers tcam
------------------------------------------------------------------------
TCAM-0 Registers
------------------------------------------------------------------------
  REV:     00B30103
  SIZE:    00080040
  ID:      00000000
  CCR:     00000000_F0000020

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

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

  GMR31:   FF_FFFFFFFF_FFFFFFFF
  GMR32:   FF_FFFFFFFF_FFFFFFFF
  GMR33:   FF_FFFFFFFF_FFFFFFFF

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

Related Commands

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

show controllers utilization

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 controllers utilization** command.

```
Switch> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Gi1/0/2           0                    0
Gi1/0/3           0                    0
Gi1/0/4           0                    0
Gi1/0/5           0                    0
Gi1/0/6           0                    0
Gi1/0/7           0                    0
<output truncated>

Gi2/0/1           0                    0
Gi2/0/2           0                    0
<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 gigabitethernet1/0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

Table 2-21 defines the field descriptions in the output.

Table 2-21 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.
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
show controllers ethernet-controller	Displays the interface internal registers.

show diagnostic

Use the **show diagnostic** user EXEC command to display the online diagnostic test results and the supported test suites.

show diagnostic content switch [*number* | **all**] [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic post [|{**begin** | **exclude** | **include**} *expression*]

show diagnostic result switch [*number* | **all**] [**detail** | **test** {*name* | *test-id* | *test-id-range* | **all**} [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

show diagnostic schedule switch [*number* | **all**] [| {**begin** | **exclude** | **include**} *expression*]

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

show diagnostic switch [*number* | **all**] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

content	Display test information including the test ID, the test attributes, and the supported coverage test levels for specific tests and for switches.
switch [*number* | **all**]	When entering the **content**, **result**, **schedule**, and **switch** keywords, you can specify the switches by using one of these options. • (Optional) Use the *number* parameter to display test information for a specific switch. The switch number is the stack member. If the switch is a standalone switch, the switch number is 1. If the switch is a stack master or a stack member, the range is 1 to 9, depending on the switch member numbers in the stack. • (Optional) Use the **all** keyword to display all the test information for the switch or the switch stack. The *number* and **all** options are supported only on the Catalyst Switch Module 3110. Use the **show diagnostic switch** [*number* | **all**] command to display the diagnostic test results for the switch or the switch stack. For information about this parameter and the **result** keyword, see the “Usage Guidelines” section.
post	Display the power-on self-test (POST) results.
result	Display the diagnostic test results.
detail	(Optional) Display the detailed test results.
test	(Optional) Specify the test results to display: • *name*—Enter the name of the diagnostic test to display results only for this test. • *test-id*—Enter the test ID number to display results only for this test. • *test-id-range*—Enter the range of test ID numbers to display results only for these tests. • **all**—Enter this keyword to display results for all the tests.
schedule	Display the scheduled diagnostic tests.

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

Defaults

This command has no default setting.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

The **show diagnostic post** command output is the same as the **show post** command output.

In switch stacks, if you do not enter the **switch** *number* parameter with the **content**, **result**, **schedule**, and **switch** keywords, information for all stack members is displayed.

On the Catalyst Switch Module 3110, the **show diagnostic result switch** [*number* | **all**] [**detail**] command output is the same as the **show diagnostic switch** [*number* | **all**] [**detail**] command output.

On the Catalyst Switch Module 3012, the **show diagnostic result** [**detail**] command output is the same as the **show diagnostic switch** [**detail**] command output.

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

Examples

This example shows how to display the online diagnostics that are configured on all the switches in a stack:

```
Switch> show diagnostic content switch all
Switch 1:
Diagnostics test suite attributes:
B/* - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
D/N/* - Disruptive test / Non-disruptive test / NA
S/* - Only applicable to standby unit / NA
X/* - Not a health monitoring test / NA
F/* - Fixed monitoring interval test / NA
E/* - Always enabled monitoring test / NA
A/I - Monitoring is active / Monitoring is inactive
R/* - Switch will reload after test list completion / NA
P/* - will partition stack / NA
Test Interval Thre-
ID Test Name Attributes day hh:mm:ss.ms shold
==== ================================== ============ ============== =====
1) TestPortAsicStackPortLoopback ---> B*N****I** not configured n/a
2) TestPortAsicLoopback ------------> B*D*X**IR* not configured n/a
3) TestPortAsicCam -----------------> B*D*X**IR* not configured n/a
```

```
4) TestPortAsicRingLoopback --------> B*D*X**IR* not configured n/a
5) TestMicRingLoopback -------------> B*D*X**IR* not configured n/a
6) TestPortAsicMem -----------------> B*D*X**IR* not configured n/a
```

This example shows how to display the running tests in a switch stack:

```
Switch> show diagnostic status
<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics
====== ================================= =============================== ======
Card   Description                       Current Running Test            Run by
------ --------------------------------- ---------------------           ------
1                                         N/A                             N/A
2                                         TestPortAsicStackPortLoopback   <OD>
                                          TestPortAsicLoopback            <OD>
                                          TestPortAsicCam                 <OD>
                                          TestPortAsicRingLoopback        <OD>
                                          TestMicRingLoopback             <OD>
                                          TestPortAsicMem                 <OD>
3                                         N/A                             N/A
4                                         N/A                             N/A
====== ================================= =============================== ======

<output truncated>
```

This example shows how to display the online diagnostic test schedule for a nonstacking-capable switch:

```
Switch> show diagnostic schedule
Current Time = 14:39:49 PST Tue Jul 5 2005
Diagnostic for Switch 1:
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
```

This example shows how to display the detailed switch results for all the switches in stack. You can also use the **show diagnostic result switch all detail** command to display these results.

```
Switch> show diagnostic switch all detail
Switch 1:   SerialNo : CAT1007R044

  Overall diagnostic result: PASS

  Test results: (. = Pass, F = Fail, U = Untested)

  ___________________________________________________________________________

    1) TestPortAsicStackPortLoopback ---> .

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 19
          Last test execution time ----> Mar 01 1993 00:21:46
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> Mar 01 1993 00:21:46
          Total failure count ---------> 0
          Consecutive failure count ---> 0
  ___________________________________________________________________________

    2) TestPortAsicLoopback ------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
 ___________________________________________________________________________

    3) TestPortAsicCam -----------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
 ___________________________________________________________________________


    4) TestPortAsicRingLoopback --------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
___________________________________________________________________________

    5) TestMicRingLoopback -------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
___________________________________________________________________________

    6) TestPortAsicMem -----------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
__________________________________________________________________________

    7) TestInlinePwrCtlr ---------------> U

          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 0
          Last test execution time ----> n/a
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> n/a
          Total failure count ---------> 0
          Consecutive failure count ---> 0
```

Related Commands

Command	Description
diagnostic monitor	Configures teh health-monitoring diagnostic test.
diagnostic schedule	Sets the scheduling of test-based online diagnostic testing.
diagnostic start	Starts the online diagnostic test.

show dot1q-tunnel

Use the **show dot1q-tunnel** user EXEC command to display information about IEEE 802.1Q tunnel ports.

show dot1q-tunnel [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Specify the interface for which to display IEEE 802.1Q tunneling information. Valid interfaces include physical ports and port channels.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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

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

```
Switch> show dot1q-tunnel
dot1q-tunnel mode LAN Port(s)
-----------------------------
Gi1/0/1
Gi1/0/2
Gi1/0/3
Gi1/0/6
Po2

Switch> show dot1q-tunnel interface gigabitethernet1/0/1
dot1q-tunnel mode LAN Port(s)
-----------------------------
Gi1/0/1
```

Related Commands

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

show dot1x

Use the **show dot1x** user 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**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all [**summary**]	(Optional) Display the IEEE 802.1x status for all ports.
interface *interface-id*	(Optional) Display the IEEE 802.1x status for the specified port (including type, stack member [Catalyst Switch Module 3110 only], module, and port number).
details	(Optional) Display the IEEE 802.1x interface details.
statistics	(Optional) Display IEEE 802.1x statistics for the specified port.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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)
```

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* appear.

Examples

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

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

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
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

<output truncated>
```

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

```
Switch> show dot1x all summary
Interface       PAE     Client          Status
--------------------------------------------------------
Gi2/0/1         AUTH    none            UNAUTHORIZED
Gi2/0/2         AUTH    00a0.c9b8.0072  AUTHORIZED
Gi2/0/3         AUTH    none            UNAUTHORIZED
```

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

```
Switch> show dot1x interface gigabitethernet1/0/2
Dot1x Info for GigabitEthernet1/0/2
-----------------------------------
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** user EXEC command:

```
Switch# show dot1x interface gigabitethernet1/0/2 details
Dot1x Info for GigabitEthernet1/0/2
-----------------------------------
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** commmand when a port is assigned to a guest VLAN and the host mode changes to multiple-hosts mode:

```
Switch# show dot1x interface gigabitethernet1/0/1 details
Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
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.

```
Switch> show dot1x interface gigabitethernet1/0/2 statistics
Dot1x Authenticator Port Statistics for GigabitEthernet1/0/2
--------------------------------------------
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 2-22 describes the fields in the display.

Table 2-22 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.
LastRxSrcMac	Source MAC address carried in the most recently received EAPOL frame.

Related Commands

Command	Description
dot1x default	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*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, stack member (Catalyst Switch Module 3110 only), module, and port number).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

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

Related Commands

Command	Description
show interfaces trunk	Displays interface trunking information.

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

Syntax Description

registrations	Display EAP registration information.
method *name*	(Optional) Display EAP method registration information.
transport *name*	(Optional) Display EAP transport registration information.
sessions	Display EAP session information.
credentials *name*	(Optional) Display EAP method registration information.
interface *interface-id*	(Optional) Display the EAP information for the specified port (including type, stack member (Catalyst Switch Module 3110 only), module, and port number).
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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* appear.

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
    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 user 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-AuthenticaInterface:               Gi1/0/1
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-AuthenticaInterface:               Gi1/0/2
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 gigabitethernet1/0/1
Role:                    Authenticator   Decision:                Fail
Lower layer:             Dot1x-AuthenticaInterface:               Gi1/0/1
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
clear eap	Clears EAP session information for the switch or for the specified port.

show env

Use the **show env** user EXEC command to display fan, temperature, and power information for the switch or the switch stack.

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

Syntax Description

all	Display the fan and temperature environmental status and the status of the internal power supplies.
stack [*switch-number*]	Display all environmental status for each switch in the stack or for the specified switch. The range is 1 to 9, depending on the switch member numbers in the stack. This keyword is supported only on the Catalyst Switch Module 3110.
temperature	Display the switch temperature status.
temperature status	(Optional) Display the switch internal temperature (not the external temperature) and the threshold values.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

On a Catalyst Switch Module 3110, use the **show env** user EXEC command to display the information for the switch being accessed—a standalone switch or the stack master. Use this command with the **stack** and **switch** keywords to display all information for the stack or for the specified stack member.

If you enter the **show env temperature status** command, the command output shows the switch temperature state and the threshold level.

You can also use the **show env temperature** command to display the switch temperature status. The command output shows the green and yellow states as *OK* and the red state as *FAULTY.* If you enter the **show env all** command, the command output is the same as the **show env temperature status** 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 an example of output from the **show env all** command on a standalone switch:

```
Switch> show env all
TEMPERATURE is OK
Temperature Value: 45 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 67 Degree Celsius
Red Threshold    : 77 Degree Celsius

POWER is OK
```

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

```
Switch> show env stack
SWITCH: 1
FAN is OK
TEMPERATURE is OK
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 65 Degree Celsius
Red Threshold    : 75 Degree Celsius
POWER is OK
RPS is AVAILABLE

<output truncated>
```

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

```
Switch> show env stack 3
SWITCH: 3
FAN is OK
TEMPERATURE is OK
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 65 Degree Celsius
Red Threshold    : 75 Degree Celsius
POWER is OK
RPS is AVAILABLE
```

This example shows how to display the temperature value, state, and the threshold values on a standalone switch. Table 2-23 describes the temperature states in the command output.

```
Switch> show env temperature status
Temperature Value: 45 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 67 Degree Celsius
Red Threshold    : 77 Degree Celsius
```

Table 2-23 States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

show errdisable detect

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

The error-disable reasons in the command output are listed in alphabetical order. The mode column shows how error disable is configured for each feature.

You can configure error-disabled detection in these modes:

- port mode—The entire physical port is error disabled if a violation occurs.
- vlan mode—The VLAN is error disabled if a violation occurs.
- port/vlan mode—The entire physical port is error disabled on some ports and per-VLAN error disabled on other ports.

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
storm-control        Enabled      port
udld                 Enabled      port
vmps                 Enabled      port
```

Related Commands

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

show errdisable flap-values

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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. See the "Examples" section for an example of the display.

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

Examples

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

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

Related Commands

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

show errdisable recovery

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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)
---------    -----------------    --------------
Gi1/0/2      link-flap             279
```

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

Related Commands

Command	Description
errdisable recovery	Configures the recover mechanism variables.
show errdisable detect	Displays error-disabled detection status.
show errdisable flap-values	Displays error condition recognition information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show etherchannel

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

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

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 48.
detail	Display detailed EtherChannel information.
load-balance	Display the load-balance or frame-distribution scheme among ports in the port channel.
port	Display EtherChannel port information.
port-channel	Display port-channel information.
protocol	Display the protocol that is being used in the EtherChannel.
summary	Display a one-line summary per channel-group.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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).

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

Examples

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

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

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

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

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

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

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

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

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

Ports in the Port-channel:

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

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

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

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

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

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

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

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

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

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

Ports in the Port-channel:

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

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

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

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

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

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates the port channel.

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 [**append** | **begin** | **exclude** | **include** | {[**redirect** | **tee**] *url*} *expression*]

Syntax Description

| append	(Optional) Append redirected output to a specified URL
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
| redirect	(Optional) Copy output to a specified URL.
| tee	(Optional) Copy output to a specified URL.
expression	Expression in the output to use as a reference point.
url	Specified URL where output is directed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

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

Examples

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
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Create a web authentication fallback profile.
ip admission	Enable web authentication on a switch port
ip admission name proxy http	Enable web authentication globally on a switch
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

show flowcontrol

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

show flowcontrol [**interface** *interface-id* | **module** *number*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Display the flow control status and statistics for a specific interface.
module *number*	(Optional) Display the flow control status and statistics for all interfaces on the switch or specified stack member. On the Catalyst Switch Module 3110, the range is 1 to 9. On the Catalyst Switch Module 3012, the only valid module number is 1. This option is not available if you have entered a specific interface ID.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

Use this command to display the flow control status and statistics on the switch or for a specific interface.

Use the **show flowcontrol** command to display information about all the switch interfaces. For a standalone switch, the output from the **show flowcontrol** command is the same as the output from the **show flowcontrol module** *number* command.

Use the **show flowcontrol interface** *interface-id* command to display information about a specific interface.

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

Examples

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

```
Switch> show flowcontrol
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi2/0/1    Unsupp.  Unsupp.  off      off         0       0
Gi2/0/2    desired  off      off      off         0       0
Gi2/0/3    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 gigabitethernet2/0/2
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi2/0/2    desired  off      off      off         0       0
```

Related Commands

Command	Description
flowcontrol	Sets the receive flow-control state for an interface.

show idprom

Use the **show idprom** user EXEC command to display the IDPROM information for the specified interface.

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

This command applies only to 10-Gigabit Ethernet interfaces.

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

Examples

This is an example of output from the **show idprom interface tengigabitethernet1/0/1** command for the 10-Gigabit Ethernet interface.

```
Switch# show idprom interface tengigabitethernet1/0/1
X2 Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
 X2 MSA Version supported :0xA
 NVR Size in bytes :0x100
 Number of bytes used :0x100
 Basic Field Address :0xB
 Customer Field Address :0x77
 Vendor Field Address :0xA7
 Extended Vendor Field Address :0x100
 Reserved :0x0
 Transceiver type :0x2 =X2
 Optical connector type :0x0 =Unspecified
 Bit encoding :0x1 =NRZ
 Normal BitRate in multiple of 1M b/s :0x2848
 Protocol Type :0x1 =10GgE

Standards Compliance Codes :
 10GbE Code Byte 0 :0x0 =Unspecified
 10GbE Code Byte 1 :0x0
 SONET/SDH Code Byte 0 :0x0
 SONET/SDH Code Byte 1 :0x0
 SONET/SDH Code Byte 2 :0x0
 SONET/SDH Code Byte 3 :0x0
 10GFC Code Byte 0 :0x0
 10GFC Code Byte 1 :0x0
 10GFC Code Byte 2 :0x0
 10GFC Code Byte 3 :0x0
 Transmission range in 10m :0x0
Fibre Type :
 Fibre Type Byte 0 :0x0 =Unspecified
 Fibre Type Byte 1 :0x0 =Unspecified

Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0
Package Identifier OUI :0xC09802
Transceiver Vendor OUI :0x3400B01
Transceiver vendor name :CISCO-OPNEXT,INC
Part number provided by transceiver vendor :TRTC010EN-BMC
Revision level of part number provided by vendor :00
Vendor serial number :OSA093900JK
Vendor manufacturing date code :2005092800

Reserved1 : 01 01 20 04 00 01 00
Basic Field Checksum :0x63

Customer Writable Area :
 0x00: 58 32 2D 31 30 47 42 2D 43 58 34 20 20 20 20 20
 0x10: 20 56 30 31 20 4F 53 41 30 39 33 39 30 30 4A 4B
 0x20: 31 30 2D 32 31 30 35 2D 30 31 20 20 41 30 20 20
Vendor Specific :
 0x00: 1F 01 1C 02 00 00 00 00 00 00 00 00 00 00 00 00
 0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x30: 00 00 01 00 11 B3 39 9F 5A 51 52 C3 2B 93 E2 A3
 0x40: 19 81 34 33 16 00 00 00 00 00 00 00 00 00 AC 76
 0x50: 37 FF 00 00 00 00 00 00 00
 F8-FF-FB, 3F-0F, 01-00
```

Related Commands

Command	Description
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware, interface internal registers, or port ASIC information.

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** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** [**backup** | **module** *number*] [**module** *number*] | **transceiver** {**tengigabitethernet** *interface-id*} | **properties** | **detail** [**module** *number*] | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Valid interfaces include physical ports (including type, stack member [Catalyst Switch Module 3110 only], module, and port number) and port channels. The port-channel range is 1 to 48.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Display accounting information on the interface, including active protocols and input and output packets and octets. **Note** The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(Optional) Display the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module *number*	(Optional) Display **capabilities**, **switchport** configuration, or **transceiver** characteristics (depending on preceding keyword) of all interfaces on the switch or specified stack member. On the Catalyst Switch Module 3110, the range is 1 to 9. On the Catalyst Switch Module 3012, the only valid module number is 1. This option is not available if you entered a specific interface ID.
counters	(Optional) See the **show interfaces counters** command.
description	(Optional) Display the administrative status and description set for an interface.
etherchannel	(Optional) Display interface EtherChannel information.
flowcontrol	(Optional) Display interface flowcontrol information
private-vlan mapping	(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 feature set.
pruning	(Optional) Display interface trunk VTP pruning information.
stats	(Optional) Display the input and output packets by switching path for the interface.
status	(Optional) Display the status of the interface.
err-disabled	(Optional) Display interfaces in error-disabled state.
switchport	(Optional) Display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
backup	(Optional) Display Flex Link backup interface configuration and status for the specified interface or all interfaces on the switch or the stack.

trunk	Display interface trunk information. If you do not specify an interface, only information for active trunking ports appears.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.
12.2(46)SE	The **tengigabitethernet** *interface-id* **transceiver detail** keywords were added.

Usage Guidelines

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

- On Catalyst Switch Module 3110, use the **show interface capabilities module** *number* command to display the capabilities of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.
- On Catalyst Switch Module 3110, use the **show interface capabilities module 1** command to display the capabilities of all interfaces on the switch. Any other number is invalid.
- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- On Catalyst Switch Module 3110, use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.
- On Catalyst Switch Module 3110, use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces on the switch.
- On Catalyst Switch Module 3110, use the **show interface switchport module** *number* command to display the switch port characteristics of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.
- On Catalyst Switch Module 3110, use the **show interface switchport module 1** to display the switch port characteristics of all interfaces on the switch. Any other number is invalid.

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

Examples

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

```
Switch# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2 packets input, 1040 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     4 packets output, 1040 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

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

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

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

<output truncated>
```

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

```
Switch# show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model:                WS-CBS3110G
Type:                   10/100/1000BaseTX
  Speed:                  10,100,1000,auto
  Duplex:                 full,auto
  Trunk encap. type:      802.1Q,ISL
  Trunk mode:             on,off,desirable,nonegotiate
  Channel:                yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:            rx-(off,on,desired),tx-(none)
  Fast Start:             yes
  QoS scheduling:         rx-(not configurable on per port basis),tx-(4q2t)
  CoS rewrite:            yes
  ToS rewrite:            yes
  UDLD:                   yes
  Inline power:           no
  SPAN:                   source/destination
  PortSecure:             yes
  Dot1x:                  yes
```

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

```
Switch# show interfaces gigabitethernet1/0/2 description
Interface Status         Protocol Description
Gi1/0/2     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 private-vlan mapping** command when the private-VLAN primary VLAN is VLAN 10 and the secondary VLANs are VLANs 501 and 502:

```
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

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 gigibitethernet1/0/2 pruning
Port    Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port    Vlans traffic requested of neighbor
Gi1/0/2   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
Gi1/0/1                      connected    routed     a-half  a-100 10/100/1000BaseTX
Gi1/0/2                      notconnect   121,40       auto   auto 10/100/1000BaseTX
Gi1/0/3                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/4                      notconnect   18           auto   auto Not Present
Gi1/0/5                      connected    121        a-full a-1000 10/100/1000BaseTX
Gi1/0/6                      connected    122,11     a-full a-1000 10/100/1000BaseTX

<output truncated>
Gi2/0/1                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi2/0/2                      notconnect   1            auto   auto unsupported

<output truncated>
```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 12 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25.

```
Switch# show interfaces gigabitethernet1/0/12 status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/12                     connected    20,25      a-full  a-100 10/100BaseTX
```

In this example, port 10 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20.

```
Switch# show interfaces gigabitethernet1/0/10 status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/10                     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
Gi1/0/2                      err-disabled gbic-invalid
Gi2/0/3                      err-disabled dtp-flap
```

This is an example of output from the **show interfaces switchport** command for a port. Table 2-24 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 gigabitethernet1/0/1 switchport
Name: Gi1/0/1
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 2-24 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.

Table 2-24 show interfaces switchport Field Descriptions (continued)

Field	Description
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 interface gigabitethernet1/0/2 switchport
Name: Gi1/0/2
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
     ------------------------------------------------------------
     Gi1/0/1             Gi1/0/2             Active Up/Backup Standby
     Gi3/0/3             Gi4/0/5             Active Down/Backup Up
     Po1                 Po2                 Active Standby/Backup Up
```

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

```
Switch# show interfaces gigibitethernet1/0/2 pruning
Port    Vlans pruned for lack of request by neighbor
```

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

```
Switch(config)# interface gigabitethernet 2/0/6
Switch(config-if)# switchport backup interface gigabitethernet 2/0/8 prefer vlan
60,100-120
```

When both interfaces are up, Gi2/0/8 forwards traffic for VLANs 60, 100 to 120, and Gi2/0/6 will forward traffic for VLANs 1 to 50.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Up

Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 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 Gi2/0/6 goes down, Gi2/0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Down/Backup Up

Vlans on Interface Gi 2/0/6:
Vlans on Interface Gi 2/0/8: 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 Gi2/0/6 comes up, then VLANs preferred on this interface are blocked on the peer interface Gi2/0/8 and forwarded on Gi2/0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Up

Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

This is an example of out put from the **show interfaces switchport backup** command when a Flex Link interface goes down (LINK_DOWN), and VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi2/0/6 goes down, Gi2/0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

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

```
Switch# show interfaces gigabitethernet1/0/1 trunk
Port          Mode         Encapsulation  Status        Native vlan
Gi1/0/1      auto         negotiate      trunking      1

Port          Vlans allowed on trunk
Gi1/0/1      1-4094

Port          Vlans allowed and active in management domain
Gi1/0/1      1-4

Port          Vlans in spanning tree forwarding state and not pruned
Gi1/0/1       1-4
```

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

```
Switch# show interfaces gigabitethernet1/0/1 transceiver properties
Name : Gi1/0/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
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 gigabitethernet2/0/3 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.

                            High Alarm  High Warn  Low Warn   Low Alarm
        Temperature         Threshold   Threshold  Threshold  Threshold
Port     (Celsius)          (Celsius)   (Celsius)  (Celsius)  (Celsius)
------- ------------------  ----------  ---------  ---------  ---------
Gi2/0/3 41.5                110.0       103.0      -8.0       -12.0
```

```
                              High Alarm  High Warn  Low Warn   Low Alarm
         Voltage              Threshold   Threshold  Threshold  Threshold
Port     (Volts)              (Volts)     (Volts)    (Volts)    (Volts)
-------  ---------------      ----------  ---------  ---------  ---------
Gi2/0/3  3.20                 4.00        3.70       3.00       2.95

                              High Alarm  High Warn  Low Warn   Low Alarm
         Current              Threshold   Threshold  Threshold  Threshold
Port     (milliamperes)       (mA)        (mA)       (mA)       (mA)
-------  -----------------    ----------  ---------  ---------  ---------
Gi2/0/3  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)
-------  -----------------    ----------  ---------  ---------  ---------
Gi2/0/3  -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)
-------  -----------------    ----------  ---------  ---------  ---------
Gi2/0/3  N/A  ( -0.0) --      -0.0        -0.0       -0.0       -0.0
```

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

```
Switch# show interfaces gigabitethernet1/0/1 transceiver properties
Name : Gi1/0/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
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 gigabitethernet2/0/3 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.

                              High Alarm  High Warn  Low Warn   Low Alarm
        Temperature           Threshold   Threshold  Threshold  Threshold
Port     (Celsius)            (Celsius)   (Celsius)  (Celsius)  (Celsius)
------- ------------------    ----------  ---------  ---------  ---------
Gi2/0/3   41.5                  110.0       103.0      -8.0       -12.0

                              High Alarm  High Warn  Low Warn   Low Alarm
         Voltage              Threshold   Threshold  Threshold  Threshold
Port     (Volts)              (Volts)     (Volts)    (Volts)    (Volts)
-------  ---------------      ----------  ---------  ---------  ---------
Gi2/0/3    3.20                 4.00        3.70       3.00       2.95

                              High Alarm  High Warn  Low Warn   Low Alarm
         Current              Threshold   Threshold  Threshold  Threshold
Port     (milliamperes)       (mA)        (mA)       (mA)       (mA)
-------  -----------------    ----------  ---------  ---------  ---------
Gi2/0/3    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)
-------  -----------------  ----------  ---------  ---------  ---------
Gi2/0/3    -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)
-------  -----------------  ----------  ---------  ---------  ---------
Gi2/0/3    N/A  ( -0.0) --    -0.0        -0.0       -0.0       -0.0
```

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

```
Switch# show interfaces tengigabitethernet1/0/1 transceiver detail
Transceiver monitoring is disabled for all interfaces.

ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or 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 calibrated.
High Alarm High Warn Low Warn Low Alarm
Temperature Threshold Threshold Threshold Threshold
Port (Celsius) (Celsius) (Celsius) (Celsius) (Celsius)
--------- ----------------- ---------- --------- --------- ---------
Te1/0/1 26.8 70.0 60.0 5.0 0.0
High Alarm High Warn Low Warn Low Alarm
Voltage Threshold Threshold Threshold Threshold
Port (Volts) (Volts) (Volts) (Volts) (Volts)
--------- --------------- ---------- --------- --------- ---------
Te1/0/1 3.15 3.63 3.63 2.97 2.97
High Alarm High Warn Low Warn Low Alarm
Current Threshold Threshold Threshold Threshold
Port (milliamperes) (mA) (mA) (mA) (mA)
--------- ----------------- ---------- --------- --------- ---------
Te1/0/1 5.0 16.3 15.3 3.9 3.2
Optical High Alarm High Warn Low Warn Low Alarm
Transmit Power Threshold Threshold Threshold Threshold
Port (dBm) (dBm) (dBm) (dBm) (dBm)
--------- ----------------- ---------- --------- --------- ---------
Te1/0/1 -1.9 1.0 0.5 -8.2 -8.5
Optical High Alarm High Warn Low Warn Low Alarm
Receive Power Threshold Threshold Threshold Threshold
Port (dBm) (dBm) (dBm) (dBm) (dBm)
------- ----------------- ---------- --------- --------- ---------
Te1/0/1 -1.4 1.0 0.5 -14.1 -15.0
```

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

```
Switch# show interfaces tengigabitethernet1/0/1 transceiver properties
Transceiver monitoring is disabled for all interfaces.

ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
Name : Te1/0/1
Administrative Speed: 10000
Administrative Duplex: full
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
```

```
Operational Speed: 10000
Operational Duplex: full
Operational Auto-MDIX: off
Media Type: 10GBase-LR
```

Related Commands

Command	Description
switchport access	Configures a port as a static-access or a dynamic-access port.
switchport block	Blocks unknown unicast or multicast traffic on an interface.
switchport backup interface	Configures Flex Links, a pair of Layer 2 interfaces that provide mutual backup.
switchport mode	Configures the VLAN membership mode of a port.
switchport mode private-vlan	Configures a port as a private-VLAN host or a promiscuous port.
switchport private-vlan	Defines private-VLAN association for a host port or private-VLAN mapping for a promiscuous port.
switchport protected	Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.

show interfaces counters

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

show interfaces [*interface-id* | **vlan** *vlan-id*] **counters** [**errors** | **etherchannel** | **module** *switch-number* | **protocol status** | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the physical interface, including type, stack member (stacking-capable switch only), module, and port number.
errors	(Optional) Display error counters.
etherchannel	(Optional) Display EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
module *switch- number*	(Optional) Display counters for the specified stack member. The range is from 1 to 9, depending upon the switch numbers in the stack. This keyword is supported only on stacking-capable switches. In this command, the **module** keyword refers to the stack member number (1 to 9). The module number that is part of the interface ID is always zero.
protocol status	(Optional) Display status of protocols enabled on interfaces.
trunk	(Optional) Display trunk counters.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
Switch# show interfaces counters
Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi1/0/1                0             0             0             0
Gi1/0/2                0             0             0             0

<output truncated>
```

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

```
Switch# show interfaces counters module 2
Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi2/0/1              520             2             0             0
Gi2/0/2              520             2             0             0
Gi2/0/3              520             2             0             0
Gi2/0/4              520             2             0             0
Gi2/0/5              520             2             0             0
Gi2/0/6              520             2             0             0
Gi2/0/7              520             2             0             0
Gi2/0/8              520             2             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
 GigabitEthernet1/0/1: Other, IP, ARP, CDP
 GigabitEthernet1/0/2: Other, IP
 GigabitEthernet1/0/3: Other, IP
 GigabitEthernet1/0/4: Other, IP
 GigabitEthernet1/0/5: Other, IP
 GigabitEthernet1/0/6: Other, IP
 GigabitEthernet1/0/7: Other, IP
 GigabitEthernet1/0/8: Other, IP
 GigabitEthernet1/0/9: Other, IP
 GigabitEthernet1/0/10: 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
Gi1/0/1                 0              0           0
Gi1/0/2                 0              0           0
Gi1/0/3             80678           4155           0
Gi1/0/4             82320            126           0
Gi1/0/5               0                0           0

<output truncated>
```

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.

show inventory

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

show inventory [*entity-name* | **raw**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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

```
Switch> show inventory
NAME: "1", DESCR: "WS-CBS3110G-S"
PID: WS-CBS3110G-S     , VID:    , SN: FHH105002F6

NAME: "2", DESCR: "WS-CBS3110X-S"
PID: WS-CBS3110X-S     , VID:    , SN: FHH10500FFF

NAME: "TenGigabitEthernet2/0/1", DESCR: "10GBase-SR"
PID: FTLX8541E2-CS     , VID: V01, SN: FNS104303F2
```

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

Syntax Description

interfaces [*interface-id*]	(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.
log	(Optional) Display the configuration and contents of the dynamic ARP inspection log buffer.
statistics [**vlan** *vlan-range*]	(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.
vlan *vlan-range*	(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.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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
  ----     -------------    ---------   ---------          ----------
     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
 ---------------  -----------     ----------    --------------
 Gi1/0/1          Untrusted               15                 1
 Gi1/0/2          Untrusted               15                 1
 Gi1/0/3          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 gigabitethernet1/0/1
 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi1/0/1          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
----------  ----  --------------  ---------------  ---------  -----------  ----
Gi1/0/1     5     0003.0000.d673  192.2.10.4              5   DHCP Deny    19:39:01 UTC
Mon Mar 1 1993
Gi1/0/1     5     0001.0000.d774  128.1.9.25              6   DHCP Deny    19:39:02 UTC
Mon Mar 1 1993
Gi1/0/1     5     0001.c940.1111  10.10.10.1              7   DHCP Deny    19:39:03 UTC
Mon Mar 1 1993
Gi1/0/1     5     0001.c940.1112  10.10.10.2              8   DHCP Deny    19:39:04 UTC
Mon Mar 1 1993
Gi1/0/1     5     0001.c940.1114  173.1.1.1              10   DHCP Deny    19:39:06 UTC
Mon Mar 1 1993
Gi1/0/1     5     0001.c940.1115  173.1.1.2              11   DHCP Deny    19:39:07 UTC
Mon Mar 1 1993
Gi1/0/1     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
arp access-list	Defines an ARP ACL.
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
clear ip arp inspection statistics	Clears the dynamic ARP inspection statistics.
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
ip arp inspection vlan logging	Controls the type of packets that are logged per VLAN.
show arp access-list	Displays detailed information about ARP access lists.

show ip dhcp snooping

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

This command displays only the results of global configuration. Therefore, in this example, the circuit ID suboption appears in its default format of **vlan-mod-port**, even if a string is configured for the circuit ID.

Examples

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

```
Switch> show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
    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)
------------------------     -------     ----------------
GigabitEthernet1/0/1             yes         unlimited
GigabitEthernet1/0/2             yes         unlimited
GigabitEthernet1/0/3             no          2000
GigabitEthernet1/0/4             yes         unlimited
```

Related Commands

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

show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** user 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*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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 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    GigabitEthernet2/0/1
00:D0:B7:1B:35:DE   10.1.2.151       237         dhcp-snooping  20    GigabitEthernet2/0/2
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    GigabitEthernet2/0/1
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    GigabitEthernet2/0/2
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 gigabitethernet2/0/2
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:30:94:C2:EF:35   10.1.2.151       290         dhcp-snooping  20    GigabitEthernet2/0/2
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    GigabitEthernet2/0/1
00:00:00:00:00:02   10.1.2.151       65          dhcp-snooping  20    GigabitEthernet2/0/2
Total number of bindings: 2
```

Table 2-25 describes the fields in the **show ip dhcp snooping binding** command output:

Table 2-25 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 **Note** 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.

Related Commands

Command	Description
ip dhcp snooping binding	Configures the DHCP snooping binding database
show ip dhcp snooping	Displays the DHCP snooping configuration.

show ip dhcp snooping database

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

show ip dhcp snooping database [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 Succeded 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 Succeded 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
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
ip dhcp snooping	Enables DHCP snooping on a VLAN.
ip dhcp snooping database	Configures the DHCP snooping binding database agent or the binding file.
show ip dhcp snooping	Displays DHCP snooping information.

show ip dhcp snooping statistics

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

show ip dhcp snooping statistics [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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
```

Table 2-26 shows the DHCP snooping statistics and their descriptions:

Table 2-26 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 **no ip dhcp snooping information option allow-untrusted** 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 **ip dhcp snooping verify mac-address** 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.

Table 2-26 DHCP Snooping Statistics (continued)

DHCP Snooping Statistic	Description
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.
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
clear ip dhcp snooping	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*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

Related Commands

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

show ip igmp snooping

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

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

Syntax Description

groups	(Optional) See the **show ip igmp snooping groups** command.
mrouter	(Optional) See the **show ip igmp snooping mrouter** command.
querier	(Optional) See the **show ip igmp snooping querier** command.
vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094 (available only in privileged EXEC mode).
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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.

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

Examples

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

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              :Enabled
IGMPv3 snooping (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
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
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping last-member-query-interval	Enables the IGMP snooping configurable-leave timer.
ip igmp snooping querier	Enables the IGMP querier function in Layer 2 networks.
ip igmp snooping report-suppression	Enables IGMP report suppression.
ip igmp snooping tcn	Configures the IGMP topology change notification behavior.
ip igmp snooping tcn flood	Specifies multicast flooding as the IGMP spanning-tree topology change notification behavior.
ip igmp snooping vlan immediate-leave	Enables IGMP snooping immediate-leave processing on a VLAN.
ip igmp snooping vlan mrouter	Adds a multicast router port or configures the multicast learning method.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping groups	Displays the IGMP snooping multicast table for the switch.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
show ip igmp snooping querier	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 [**count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

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

Syntax Description

count	(Optional) Display the total number of entries for the specified command options instead of the actual entries.
dynamic	(Optional) Display entries learned by IGMP snooping.
user	Optional) Display only the user-configured multicast entries.
ip_address	(Optional) Display characteristics of the multicast group with the specified group IP address.
vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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

Examples

This is an example of output from the **show ip igmp snooping 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
-------------------------------------------------------------
1         224.1.4.4      igmp                    Gi1/0/11
1         224.1.4.5      igmp                    Gi1/0/11
2         224.0.1.40     igmp        v2          Gi1/0/14
104       224.1.4.2      igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3      igmp        v2          Gi2/0/1, Gi2/0/2
```

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
-------------------------------------------------------------
104       224.1.4.2      igmp        v2          Gi2/0/1, Gi1/0/14
104       224.1.4.3      igmp        v2          Gi2/0/1, Gi1/0/14
```

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          Gi2/0/1, Gi1/0/14
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan mrouter	Configures a multicast router port.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

show ip igmp snooping mrouter

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

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

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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 **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.

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

Examples

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

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

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan mrouter	Adds a multicast router port.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN
show ip igmp snooping groups	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** user 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**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	Optional) Display detailed IGMP querier information.
vlan *vlan-id* [**detail**]	Optional) Display IGMP querier information for the specified VLAN. The range is 1 to 1001 and 1006 to 4094. Use the **detail** keyword to display detailed information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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** user 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

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

Examples

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

```
Switch> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
---------------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

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             Fa8/0/1

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 Fa8/0/1
--------------------------------------------------------
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
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping querier	Enables the IGMP querier function in Layer 2 networks.
show ip igmp snooping	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** user 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*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

ip-address	(Optional) Display IP source bindings for a specific IP address.
mac-address	(Optional) Display IP source bindings for a specific MAC address.
dhcp-snooping	(Optional) Display IP source bindings that were learned by DHCP snooping.
static	(Optional) Display static IP source bindings.
interface *interface-id*	(Optional) Display IP source bindings on a specific interface.
vlan *vlan-id*	(Optional) Display IP source bindings on a specific VLAN.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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

Examples

This is an example of output from the **show ip 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    GigabitEthernet1/0/1
00:00:00:0A:00:0A   11.0.0.2         10000       dhcp-snooping  10    GigabitEthernet1/0/1
```

Related Commands

Command	Description
ip dhcp snooping binding	Configures the DHCP snooping binding database.
ip source binding	Configures static IP source bindings on the switch.

show ip verify source

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

show ip verify source [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	**Modification**
12.2(40)EX2	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 ip verify source** command:

```
Switch> show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi1/0/1      ip           active       10.0.0.1                         10
gi1/0/1      ip           active       deny-all                         11-20
gi1/0/2      ip           inactive-trust-port
gi1/0/3      ip           inactive-no-snooping-vlan
gi1/0/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
gi1/0/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
gi1/0/4      ip-mac       active       deny-all         deny-all        12-20
gi1/0/5      ip-mac       active       10.0.0.3         permit-all      10
gi1/0/5      ip-mac       active       deny-all         permit-all      11-20
```

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

- On the Gigabit Ethernet 1/0/1 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 1/0/2 interface is configured as trusted for DHCP snooping.
- On the Gigabit Ethernet 1/0/3 interface, DHCP snooping is not enabled on the VLANs to which the interface belongs.

- On the Gigabit Ethernet 1/0/4 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 1/0/5 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 gigabitethernet1/0/6
IP source guard is not configured on the interface gi1/0/6.
```

Related Commands

Command	Description
ip verify source	Enables IP source guard on an interface.

show ipc

Use the **show ipc** user EXEC command to display Interprocess Communications Protocol (IPC) configuration, status, and statistics on a switch stack or a standalone switch.

show ipc {**mcast** {**appclass** | **groups** | **status**} | **nodes** | **ports** [**open**] | **queue** | **rpc** | **session** {**all** | **rx** | **tx**} [**verbose**] | **status** [**cumlulative**] | **zones**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

mcast {**appclass** | **groups** | **status**}	Display the IPC multicast routing information. The keywords have these meanings: • **appclass**—Display the IPC multicast application classes. • **groups**—Display the IPC multicast groups. • **status**—Display the IPC multicast routing status.
nodes	Display participating nodes.
ports [**open**]	Display local IPC ports. The keyword has this meaning: • **open**—(Optional) Display only the open ports.
queue	Display the contents of the IPC transmission queue.
rpc	Display the IPC remote-procedure statistics.
session {**all** | **rx** | **tx**}	Display the IPC session statistics (available only in privileged EXEC mode). The keywords have these meanings: • **all**—Display all the session statistics. • **rx**—Display the sessions statistics for traffic that the switch receives • **tx**—Display the sessions statistics for traffic that the switch forwards.
verbose	(Optional) Display detailed statistics (available only in privileged EXEC mode).
status [**cumlulative**]	Display the status of the local IPC server. The keyword has this meaning: • **cumlulative**—(Optional) Display the status of the local IPC server since the switch was started or restarted.
zones	Display the participating IPC zones. The switch supports a single IPC zone.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 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  Last
                                    Sent  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
   10000.7     Unicast    MDFS RP:Statistics
     port_index = 0  type = Unreliable      last sent = 0     last heard = 0
     Msgs requested = 180  Msgs returned = 180

   10000.8     Unicast    Slot 1 :MDFS.control.RIL
     port_index = 0  type = Reliable        last sent = 0     last heard = 0
     Msgs requested = 0    Msgs returned = 0

Rx Sessions:
Port ID        Type       Name
   10000.7     Unicast    MDFS RP:Statistics
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
     No of msgs requested = 180   Msgs returned = 180

   10000.8     Unicast    Slot 1 :MDFS.control.RIL
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 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
clear ipc	Clears the IPC multicast routing statistics.

show ipv6 access-list

Use the **show ipv6 access-list** user EXEC command to display the contents of all current IPv6 access lists.

show ipv6 access-list [*access-list-name*]

Note This command is supported only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

access-list-name	(Optional) Name of access list.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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** {**default** | **vlan**) global configuration command and reload the switch.

Examples

The following output from the **show ipv6 access-list** command shows IPv6 access lists named inbound and outbound:

```
Switch# 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 2-27 describes the significant fields shown in the display.

Table 2-27 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 2-27 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
clear ipv6 access-list	Resets the IPv6 access list match counters. For syntax information, go to http://www.cisco.com/en/US/products/ps5845/products_command_reference_chapter09186a008027e846.html#wp1238563
ipv6 access-list	Defines an IPv6 access list and puts the switch into IPv6 access-list configuration mode.
sdm prefer	Configures an SDM template to optimize system resources based on how the switch is being used.

show ipv6 dhcp conflict

Use the **show ipv6 dhcp conflict** privileged EXEC commandto display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client.

show ipv6 dhcp conflict

Note This command is available only if the switch stack or standalone switch is running the advanced IP services feature set and you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(46)SE	This command was introduced.

Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** {**default** | **vlan**) global configuration command, and reload the switch.

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.

Examples

This is an example of the output from the **show ipv6 dhcp conflict** command:

```
Switch# show ipv6 dhcp conflict
Pool 350, prefix 2001:1005::/48
        2001:1005::10
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 pool and enters DHCPv6 pool configuration mode.
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.

show ipv6 mld snooping

Use the **show ipv6 mld snooping** user EXEC command to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.

show ipv6 mld snooping [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Note This command is supported only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** {**default** | **vlan**) global configuration command and reload the switch.

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

Examples

This is an example of output from the **show ipv6 mld snooping vlan** 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
ipv6 mld snooping	Enables and configures MLD snooping on the switch or on a VLAN.
sdm prefer	Configures an SDM template to optimize system resources based on how the switch is being used.

show ipv6 mld snooping address

Use the **show ipv6 mld snooping address** user EXEC command to display all or specified IP Version 6 (IPv6) multicast address information maintained by Multicast Listener Discovery (MLD) snooping.

show ipv6 mld snooping address [[**vlan** *vlan-id*] [*ipv6 address*]] [**vlan** *vlan-id*] [**count** | **dynamic** | **user**] [| {**begin** | **exclude** | **include**} *expression*]

Note This command is supported only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN about which to show MLD snooping multicast address information. The VLAN ID range is 1 to 1001 and 1006 to 4094.
ipv6-multicast-address	(Optional) Display information about the specified IPv6 multicast address. This keyword is only available when a VLAN ID is entered.
count	(Optional) Display the number of multicast groups on the switch or in the specified VLAN.
dynamic	(Optional) Display MLD snooping learned group information.
user	(Optional) Display MLD snooping user-configured group information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

Use this command to display IPv6 multicast address information.

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.

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** {**default** | **vlan**) global configuration command and reload the switch.

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

Examples

This is an example of output from the **show snooping address** user EXEC command:

Switch> **show ipv6 mld snooping address**

```
Vlan Group   Type Version Port List
-------------------------------------------------------------
2    FF12::3 user         Gi1/0/2, Gi2/0/2, Gi3/0/1,Gi3/0/3
```

This is an example of output from the **show snooping address count** user EXEC command:

```
Switch> show ipv6 mld snooping address count
Total number of multicast groups: 2
```

This is an example of output from the **show snooping address user** user EXEC command:

```
Switch> show ipv6 mld snooping address user
Vlan Group  Type Version Port List
-------------------------------------------------------------
2    FF12::3 user  v2    Gi1/0/2, Gi2/0/2, Gi3/0/1,Gi3/0/3
```

Related Commands

Command	Description
ipv6 mld snooping vlan	Configures IPv6 MLD snooping on a VLAN.
sdm prefer	Configures an SDM template to optimize system resources based on how the switch is being used.

show ipv6 mld snooping mrouter

Use the **show ipv6 mld snooping mrouter** user EXEC command to display dynamically learned and manually configured IP version 6 (IPv6) Multicast Listener Discovery (MLD) router ports for the switch or a VLAN.

show ipv6 mld snooping mrouter [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Note This command is supported only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

Use this command to display MLD snooping router ports for the switch or for a specific VLAN.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** {**default** | **vlan**) global configuration command and reload the switch.

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

Examples

This is an example of output from the **show ipv6 mld snooping mrouter** 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    Gi1/0/11(dynamic)
  72    Gi1/0/11(dynamic)
 200    Gi1/0/11(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    Gi1/0/11(dynamic)
```

Related Commands

Command	Description
ipv6 mld snooping	Enables and configures MLD snooping on the switch or on a VLAN.
ipv6 mld snooping vlan mrouter interface *interface-id* **|** **static** *ipv6-multicast-address* **interface** *interface-id*]	Configures multicast router ports for a VLAN.
sdm prefer	Configures an SDM template to optimize system resources based on how the switch is being used.

show ipv6 mld snooping querier

Use the **show ipv6 mld snooping querier** user EXEC command to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping querier-related information most recently received by the switch or the VLAN.

show ipv6 mld snooping querier [**vlan** *vlan-id*] [**detail**] [**|** {**begin** | **exclude** | **include**} *expression*]

Note This command is supported only if you have configured a dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Display MLD snooping detailed querier information for the switch or for the VLAN.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

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.

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** {**default** | **vlan**) global configuration command and reload the switch.

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

Examples

This is an example of output from the **show ipv6 mld snooping querier** command:

```
Switch> show ipv6 mld snooping querier
Vlan      IP Address               MLD Version Port
-------------------------------------------------------------
2         FE80::201:C9FF:FE40:6000 v1          Gi3/0/1
```

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           Gi3/0/1
```

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 : Gi3/0/1
Max response time : 1000s
```

Related Commands

Command	Description
ipv6 mld snooping	Enables and configures IPv6 MLD snooping on the switch or on a VLAN.
ipv6 mld snooping last-listener-query-count	Configures the maximum number of queries that the switch sends before aging out an MLD client.
ipv6 mld snooping last-listener-query-interval	Configures the maximum response time after sending out a query that the switch waits before deleting a port from the multicast group.
ipv6 mld snooping robustness-variable	Configures the maximum number of queries that the switch sends before aging out a multicast address when there is no response.
sdm prefer	Configures an SDM template to optimize system resources based on how the switch is being used.
ipv6 mld snooping	Enables and configures IPv6 MLD snooping on the switch or on a VLAN.

show ipv6 route updated

Use the **show ipv6 route updated command in** user EXEC command to display the current contents of the IPv6 routing table.

show ipv6 route [*protocol*] **updated** [**boot-up**] {*hh:mm* | *day*{*month* [*hh:mm*]} [{*hh:mm* | *day*{*month* [*hh:mm*]}] [| {**begin** | **exclude** | **include**} *expression*]

This command is supported only on the Catalyst Switch Module 3110.

Syntax Description

protocol	(Optional) Displays routes for the specified routing protocol using any of these keywords: • **bgp** • **isis** • **ospf** • **rip** or displays routes for the specified type of route using any of these keywords: • **connected** • **local** • *static* • **interface** *interface id*
boot-up	Display the current contents of the IPv6 routing table.
hh:mm	Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colons (:). For example, enter **13:32**
day	Enter the day of the month. The range is from 1 to 31.
month	Enter the month in upper case or lower case letters. You can enter the full name of the month, such as **January** or **august**, or the first three letters of the month, such as **jan** or **Aug**.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

Use the **show ipv6 route** privileged EXEC command to display the current contents of the IPv6 routing table.

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 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, GigabitEthernet1/0/1
Last updated 10:31:10 27 February 2007
R 2004::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/0/2
Last updated 17:23:05 22 February 2007
R 4000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/0/3
Last updated 17:23:05 22 February 2007
R 5000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/0/4
Last updated 17:23:05 22 February 2007
R 5001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet1/0/5
Last updated 17:23:05 22 February 2007
```

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table. For syntax information, select **Cisco IOS Software > Command References for the Cisco IOS Software Releases 12.3 Mainline > Cisco IOS IPv6 Command Reference > IPv6 Commands: show ipv6 nat translations through show ipv6 protocols**

show l2protocol-tunnel

Use the **show l2protocol-tunnel** user EXEC command to display information about Layer 2 protocol tunnel ports. Displays information for interfaces with protocol tunneling enabled.

show l2protocol-tunnel [**interface** *interface-id*] [**summary**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Specify the interface for which protocol tunneling information appears. Valid interfaces are physical ports and port channels; the port channel range is 1 to 48.
summary	(Optional) Display only Layer 2 protocol summary information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

After enabling Layer 2 protocol tunneling on an access or IEEE 802.1Q tunnel port by using the **l2protocol-tunnel** interface configuration command, you 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.

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 l2protocol-tunnel** command:

```
Switch> show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

 Port       Protocol Shutdown  Drop      Encapsulation Decapsulation Drop
                    Threshold Threshold Counter       Counter       Counter
---------- --------- --------- --------- ------------- ------------- -------------
  Gi3/0/3    ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           pagp          ----      ----             0         242500
           lacp          ----      ----         24268         242640
           udld          ----      ----             0         897960
  Gi3/0/4    ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           pagp          1000      ----         24249         242700
           lacp          ----      ----         24256         242660
           udld          ----      ----             0         897960
  Gi6/0/1    cdp           ----      ----        134482        1344820
           ---           ----      ----          ----          ----          ----
           ---           ----      ----          ----          ----          ----
           pagp          1000      ----             0         242500
           lacp           500      ----             0         485320
           udld           300      ----         44899         448980
  Gi6/0/2     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         Drop             Status
                    Threshold        Threshold
                    (cdp/stp/vtp)    (cdp/stp/vtp)
                    (pagp/lacp/udld) (pagp/lacp/udld)
------- ----------- ---------------- ---------------- ----------
  Gi3/0/2  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld ----/----/----   ----/----/----
  Gi4/0/3  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld 1000/----/----   ----/----/----
  Gi4/0/4  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld 1000/ 500/----   ----/----/----
  Gi4/0/5  cdp stp vtp ----/----/----   ----/----/----   down
     ---- ---- ---- ----/----/----   ----/----/----
  Gi9/0/1  --- --- --- ----/----/----   ----/----/----   down
     pagp ---- ---- ----/----/----   1000/----/----
  Gi9/0/2  --- --- --- ----/----/----   ----/----/----   down
     pagp ---- ---- ----/----/----   1000/----/----
```

Related Commands

Command	Description
clear l2protocol-tunnel counters	Clears counters for protocol tunneling ports.
l2protocol-tunnel	Enables Layer 2 protocol tunneling for CDP, STP, or VTP packets on an interface.
l2protocol-tunnel cos	Configures a class of service (CoS) value for tunneled Layer 2 protocol packets.

show lacp

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

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

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 48.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
sys-id	Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the switch MAC address.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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**.

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

Examples

This is an example of output from the **show lacp counters** user EXEC command.

```
Switch> show lacp counters
             LACPDUs         Marker      Marker Response    LACPDUs
Port         Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group:1
Gi2/0/1      19     10       0      0        0      0         0
Gi2/0/2      14     6        0      0        0      0         0
```

Table 2-28 describes the fields in the display.

Table 2-28 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.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDUs 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
                              LACP port     Admin     Oper    Port     Port
Port        Flags   State     Priority      Key       Key     Number   State
Gi2/0/1     SA      bndl      32768         0x3       0x3     0x4      0x3D
Gi2/0/2     SA      bndl      32768         0x3       0x3     0x5      0x3D
```

Table 2-29 describes the fields in the display:

Table 2-29 show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: • – —Port is in an unknown state. • **bndl**—Port is attached to an aggregator and bundled with other ports. • **susp**—Port is in a suspended state; it is not attached to any aggregator. • **hot-sby**—Port is in a hot-standby state. • **indiv**—Port is incapable of bundling with any other port. • **indep**—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). • **down**—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports s in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Table 2-29 show lacp internal Field Descriptions (continued)

Field	Description
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port number.
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired **Note** In the list above, bit7 is the MSB and bit0 is the LSB.

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

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

Channel group 3 neighbors

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi2/0/1   32768,0007.eb49.5e80  0xC              19s        SP

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

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi2/0/2   32768,0007.eb49.5e80  0xD              15s        SP

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

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

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

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

Related Commands

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

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

Syntax Description

number	(Optional) Number of the link-state group.
detail	(Optional) Specify that detailed information appears.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	**Modification**
12.2(40)EX2	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 configuration for a group, the group is not shown as enabled or disabled.

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

Examples

This is an example of output from the **show 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 : Gi1/0/17(Dwn) Gi1/0/18(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Commands

Command	Description
link state group	Configures an interface as a member of a link-state group.
link state track	Enables a link-state group.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command.

show location

Use the **show location** user EXEC command to display location information for an endpoint.

show location admin-tag | [| {**begin** | **exclude** | **include**} *expression*]

show location civic-location {**identifier** *id number* | **interface** *interface-id* | **static** } | {**begin** | **exclude** | **include**} *expression*]

show location elin-location {**identifier** *id number* | **interface** *interface-id* | **static** } | {**begin** | **exclude** | **include**} *expression*]

Syntax Description

admin-tag	Display administrative tag or site information.
civic-location	Display civic location information.
elin-location	Display emergency location information (ELIN).
identifier *id*	Specify the ID for the civic location or the elin location. The id range is 1 to 4095.
interface *interface-id*	Display location information for the specified interface or all interfaces. Valid interfaces include physical ports.
static	Display static configuration information.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

Use the **show location** command to display location information for an endpoint.

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 location civic-location** command that displays location information for an interface:

```
Switch> show location civic interface gigabitethernet2/0/1
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                    : Gi2/0/1
--------------------------
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      : Gi2/0/2
```

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      : Gi2/0/2
--------------------------
Identifier : 2
Elin       : 18002228999
--------------------------
```

Related Commands

Command	Description
location (global configuration)	Configures the global location information for an endpoint.
location (interface configuration)	Configures the location information for an interface.

show logging

Use the **show logging** privileged EXEC command to display the on-board failure logging (OBFL) information.

show logging onboard [**module** [*switch-number*]] {{**clilog** | **environment** | **message** | **temperature** | **uptime** | **voltage**} [**continuous** | **detail** | **summary**] [**start** *hh:mm:ss day month year*] [**end** *hh:mm:ss day month year*]} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

module [*switch-number*]	(Optional) Display OBFL information about the specified switches. On stacking-capable switches, use the *switch-number* parameter to specify the switch number, which is the stack member number. If the switch is a standalone switch, the switch number is 1. If the switch is in a stack, the range is 1 to 9, depending on the switch member numbers in the stack. On nonstacking-capable switches, the *switch-number* parameter is always **1**. For more information about this parameter, see the “Usage Guidelines” section for this command.
clilog	Display the OBFL CLI commands that were entered on the standalone switch or specified stack members.
environment	Display the unique device identifier (UDI) information for the standalone switch or specified stack members and for all the connected FRU devices: the product identification (PID), the version identification (VID), and the serial number.
message	Display the hardware-related system messages generated by the standalone switch or specified stack members.
temperature	Display the temperature of the standalone switch or specified stack members.
uptime	Display the time when the standalone switch or specified stack members start, the reason the switch or specified members restart, and the length of time the standalone switch or specified stack members have been running since they last restarted.
voltage	Display the system voltages of the standalone switch or the specified switch stack members.
continuous	(Optional) Display the data in the *continuous* file.
summary	(Optional) Display the data in the *summary* file.
start *hh:mm:ss day month year*	(Optional) Display the data from the specified time and date. For more information, see the “Usage Guidelines” section.
end *hh:mm:ss day month year*	(Optional) Display the data up to the specified time and date. For more information, see the “Usage Guidelines” section.
detail	(Optional) Display both the continuous and summary data.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.

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

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

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

When OBFL is enabled, the switch records OBFL data in a continuous file that contains all of the data. The continuous file is circular. When the continuous file is full, the switch combines the data into a summary file, which is also known as a historical file. Creating the summary file frees up space in the continuous file so that the switch can write newer data to it.

When using the **module** *switch-number* parameter, follow these guidelines:

- On a stacking-capable switch, if you enter the **module** keyword but do not enter the switch number, the switch displays OBFL information about the stack members that support OBFL.
- On a nonstacking-capable switch, if you enter the **module** keyword, you must enter the *switch-number* value of **1**.

Use the **start** and **end** keywords to display data collected only during a particular time period. When specifying the **start** and **end** times, follow these guidelines:

- *hh:mm:ss*—Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colons (:). For example, enter **13:32:45**.
- *day*—Enter the day of the month. The range is from 1 to 31.
- *month*—Enter the month in upper case or lower case letters. You can enter the full name of the month, such as **January** or **august**, or the first three letters of the month, such as **jan** or **Aug**.
- *year*—Enter the year as a 4-digit number, such as 2008. The range is from 1993 to 2035.

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

Examples

This is an example of output from the **show logging onboard clilog continuous** command:

```
Switch# show logging onboard clilog continuous
--------------------------------------------------------------------------------
CLI LOGGING CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS COMMAND
--------------------------------------------------------------------------------
05/12/2006 15:33:17 show logging onboard temperature detail
05/12/2006 15:33:21 show logging onboard voltage detail
05/12/2006 15:33:32 show logging onboard poe detail
05/12/2006 16:14:09 show logging onboard temperature summary
...
<output truncated>
....
05/16/2006 13:07:53 no hw-module module logging onboard message level
05/16/2006 13:16:13 show logging onboard uptime continuous
05/16/2006 13:39:18 show logging onboard uptime summary
05/16/2006 13:45:57 show logging onboard clilog summary
--------------------------------------------------------------------------------
```

This is an example of output from the **show logging onboard message** command:

```
Switch# show logging onboard message
--------------------------------------------------------------------------------
ERROR MESSAGE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Facility-Sev-Name      | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
```

This is an example of output from the **show logging onboard status** command:

```
Switch# show logging onboard status
Devices registered with infra
                 Slot no.: 0 Subslot no.: 0, Device obfl0:
Application name clilog :
                 Path : obfl0:
                 CLI enable status  : enabled
                 Platform enable status: enabled
Application name environment :
                 Path : obfl0:
                 CLI enable status  : enabled
                 Platform enable status: enabled
Application name errmsg :
                 Path : obfl0:
                 CLI enable status  : enabled
                 Platform enable status: enabled
Application name poe :
                 Path : obfl0:
                 CLI enable status  : enabled
                 Platform enable status: enabled
Application name temperature :
                 Path : obfl0:
                 CLI enable status  : enabled
                 Platform enable status: enabled
Application name uptime :
                 Path : obfl0:
                 CLI enable status  : enabled
                 Platform enable status: enabled
```

```
Application name voltage :
                 Path : obfl0:
                 CLI enable status  : enabled
                 Platform enable status: enabled
```

This is an example of output from the **show logging onboard temperature continuous** command:

```
Switch# show logging onboard temperature continuous
--------------------------------------------------------------------------------
TEMPERATURE CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Sensor                            |   ID  |
--------------------------------------------------------------------------------
Board temperature                        1

--------------------------------------------------------------------------------
       Time Stamp   |Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS |  1    2    3    4    5    6    7    8    9   10   11   12
--------------------------------------------------------------------------------
05/12/2006 15:33:20   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 16:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 17:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 18:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 19:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 20:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 21:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 22:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 23:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 00:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 01:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 02:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 03:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 04:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 05:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 06:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 07:25:24   36   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 08:25:24   35   --   --   --   --   --   --   --   --   --   --   --
<output truncated>
```

This is an example of output from the **show logging onboard uptime summary** command:

```
Switch# show logging onboard uptime summary
--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 03/01/1993 00:03:50
Total uptime            :   0 years   0 weeks   3 days  21 hours  55 minutes
Total downtime          :   0 years   0 weeks   0 days   0 hours   0 minutes
Number of resets        : 2
Number of slot changes  : 1
Current reset reason    : 0x0
Current reset timestamp : 03/01/1993 00:03:28
Current slot            : 1
Current uptime          :   0 years   0 weeks   0 days   0 hours  55 minutes
--------------------------------------------------------------------------------
Reset  |        |
Reason | Count  |
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
```

This is an example of output from the **show logging onboard voltage summary** command:

```
Switch# show logging onboard voltage summary
--------------------------------------------------------------------------------
VOLTAGE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Number of sensors           : 8
Sampling frequency          : 60 seconds
Maximum time of storage     : 3600 minutes
--------------------------------------------------------------------------------
Sensor                           |   ID  | Maximum Voltage
--------------------------------------------------------------------------------
12.00V                            0      12.567
5.00V                             1       5.198
3.30V                             2       3.439
2.50V                             3       2.594
1.50V                             4       1.556
1.20V                             5       1.239
1.00V                             6       0.980
0.75V                             7       0.768
--------------------------------------------------------------------------------
Nominal Range                        Sensor ID

--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
```

Related Commands

Command	Description
clear logging	Removes the OBFL data in the flash memory.
hw-module module [*switch-number*] **logging onboard**	Enables OBFL.

show mac access-group

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

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

Syntax Description

interface *interface-id*	(Optional) Display the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port-channel range is 1 to 48 (available only in privileged EXEC mode).
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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-access group** user EXEC command. In this display, port 2 has the MAC access list *macl_e1* applied; no MAC ACLs are applied to other interfaces.

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

<output truncated>
```

This is an example of output from the **show mac access-group interface gigabitethernet1/0/1** command:

```
Switch# show mac access-group interface gigabitethernet1/0/1
Interface GigabitEthernet1/0/1:
   Inbound access-list is macl_e1
```

Related Commands

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

show mac address-table

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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
----    -----------       ----       -----
 All    0000.0000.0001    STATIC     CPU
 All    0000.0000.0002    STATIC     CPU
 All    0000.0000.0003    STATIC     CPU
 All    0000.0000.0009    STATIC     CPU
 All    0000.0000.0012    STATIC     CPU
 All    0180.c200.000b    STATIC     CPU
 All    0180.c200.000c    STATIC     CPU
 All    0180.c200.000d    STATIC     CPU
 All    0180.c200.000e    STATIC     CPU
 All    0180.c200.000f    STATIC     CPU
 All    0180.c200.0010    STATIC     CPU
   1    0030.9441.6327    DYNAMIC    Gi6/0/4
Total Mac Addresses for this criterion: 12
```

Related Commands

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

show mac address-table address

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table aging-time

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

If no VLAN number is specified, the aging time 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 aging-time** command:

```
Switch> show mac address-table aging-time
Vlan    Aging Time
----    ----------
   1     300
```

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

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

Related Commands

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

show mac address-table count

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table dynamic

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 dynamic** command:

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

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

Related Commands

Command	Description
clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table interface

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 interface** command:

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

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

Related Commands

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

show mac address-table learning

Use the **show mac address-table learning** user 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*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(46)SE	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** user 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
```

Related Commands

Command	Description
mac address-table learning vlan	Enables or disables MAC address learning on a VLAN.

show mac address-table move update

Use the **show mac address-table move update** user 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

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 move update** 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
clear mac address-table move update	Clears the MAC address-table move update counters.
mac address-table move update {**receive** | **transmit**}	Configures MAC address-table move update on the switch.

show mac address-table notification

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

Use the **show mac address-table notification** command without any keywords to display whether the feature is enabled or disabled, the MAC notification interval, the maximum number of entries allowed in the history table, and the history table contents.

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

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

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

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

Related Commands

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

show mac address-table static

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

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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
mac address-table static	Adds static addresses to the MAC address table.
mac address-table static drop	Enables unicast MAC address filtering and configures the switch to drop traffic with a specific source or destination MAC address.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table vlan

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.

show mls qos

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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** command when QoS is enabled and Differentiated Services Code Point (DSCP) transparency is disabled:

```
Switch> show mls qos
QoS is enabled
QoS ip packet dscp rewrite is disabled
```

This is an example of output from the **show mls qos** 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
mls qos	Enables QoS for the entire switch.

show mls qos aggregate-policer

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 aggregate-policer** 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
mls qos aggregate-policer	Defines policer parameters that can be shared by multiple classes within a policy map.

show mls qos input-queue

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 input-queue** command:

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

Related Commands

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

show mls qos interface

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

show mls qos interface [*interface-id*] [**buffers** | **queueing** | **statistics**]
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 gigabitethernet1/0/1
GigabitEthernet1/0/1
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 gigabitethernet1/0/2
GigabitEthernet1/0/2
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 gigabitethernet1/0/2 buffers
GigabitEthernet1/0/2
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 gigabitethernet1/0/2 queueing
GigabitEthernet1/0/2
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 2-30 describes the fields in this display.

```
Switch> show mls qos interface gigabitethernet1/0/2 statistics
GigabitEthernet1/0/2

  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
  dscp: outgoing
-------------------------------

  0 -  4 :    363949          0          0          0          0
  5 -  9 :         0          0          0          0          0
 10 - 14 :         0          0          0          0          0
 15 - 19 :         0          0          0          0          0
 20 - 24 :         0          0          0          0          0
 25 - 29 :         0          0          0          0          0
 30 - 34 :         0          0          0          0          0
 35 - 39 :         0          0          0          0          0
 40 - 44 :         0          0          0          0          0
 45 - 49 :         0          0          0          0          0
 50 - 54 :         0          0          0          0          0
 55 - 59 :         0          0          0          0          0
 60 - 64 :         0          0          0          0
  cos: incoming
-------------------------------

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

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

Policer: Inprofile:        0 OutofProfile:        0
```

Table 2-30 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
mls qos queue-set output buffers	Allocates buffers to a queue-set.
mls qos queue-set output threshold	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
mls qos srr-queue input bandwidth	Assigns SRR weights to an ingress queue.
mls qos srr-queue input buffers	Allocates the buffers between the ingress queues.
mls qos srr-queue input cos-map	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue input dscp-map	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
mls qos srr-queue input priority-queue	Configures the ingress priority queue and guarantees bandwidth.
mls qos srr-queue input threshold	Assigns WTD threshold percentages to an ingress queue.
mls qos srr-queue output cos-map	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
mls qos srr-queue output dscp-map	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
policy-map	Creates or modifies a policy map.
priority-queue	Enables the egress expedite queue on a port.
queue-set	Maps a port to a queue-set.
srr-queue bandwidth limit	Limits the maximum output on a port.
srr-queue bandwidth shape	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

show mls qos maps

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 03-01 03-01 03-01 03-01
   2 :    03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
   3 :    03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01 04-01
   5 :    04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
   6 :    04-01 04-01 04-01 04-01
```

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

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

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

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

Related Commands

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

show mls qos queue-set

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.nway

Examples

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

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

Related Commands

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

show mls qos vlan

Use the **show mls qos vlan** user 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

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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
policy-map	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** user EXEC command to display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch. Use the command with keywords to show a specific session, all sessions, all local sessions, or all remote sessions.

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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** user EXEC command:

```
Switch# show monitor
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/10
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** user EXEC command for local SPAN source session 1:

```
Switch# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/10
Encapsulation : Replicate
Ingress : Disabled
```

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

```
Switch# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

Related Commands

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

show mvr

Use the **show mvr** privileged EXEC command without keywords to display the current Multicast VLAN Registration (MVR) global parameter values, including whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible).

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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 mvr** command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the preceding display, the maximum number of multicast groups is fixed at 256. The MVR mode is either compatible (for 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
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **interface** and **members** keywords are appended to the command.
show mvr members	Displays all ports that are members of an MVR multicast group or, if there are no members, means the group is inactive.

show mvr interface

Use the **show mvr interface** privileged EXEC command without keywords to display the Multicast VLAN Registration (MVR) receiver and source ports. Use the command with keywords to display MVR parameters for a specific receiver port.

show mvr interface [*interface-id* [**members** [**vlan** *vlan-id*]]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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
----        ----            -------         ---------------
Gi1/0/1   SOURCE          ACTIVE/UP       DISABLED
Gi1/0/2   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 gigabitethernet1/0/2
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 gigabitethernet1/0/2 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
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr members	Displays all receiver ports that are members of an MVR multicast group.

show mvr members

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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          Gi1/0/1(d), Gi1/0/5(s)
239.255.0.2     INACTIVE        None
239.255.0.3     INACTIVE        None
239.255.0.4     INACTIVE        None
239.255.0.5     INACTIVE        None
239.255.0.6     INACTIVE        None
239.255.0.7     INACTIVE        None
239.255.0.8     INACTIVE        None
239.255.0.9     INACTIVE        None
239.255.0.10    INACTIVE        None

<output truncated>
```

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), Gi1/0/2(d), Gi1/0/3(d),
                                     Gi1/0/4(d), Gi1/0/5(s)
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **members** keyword is appended to the command.

show pagp

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

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

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 48.
counters	Display traffic information.
dual-active	Display the dual-active status.
internal	Display internal information.
neighbor	Display neighbor information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.
12.2(46)SE	The **dual-active** 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
  Gi1/0/1    45     42        0      0
  Gi1/0/2    45     41        0      0
```

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

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

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

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

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

    Channel group 1 neighbors
                Partner              Partner          Partner         Partner Group
    Port        Name                 Device ID        Port       Age  Flags   Cap.
    Gi1/0/1     switch-p2            0002.4b29.4600   Gi01//1     9s  SC      10001
    Gi1/0/2     switch-p2            0002.4b29.4600   Gi1/0/2    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
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi1/0/1   No              Switch               Gi3/0/3   N/A
Gi1/0/2   No              Switch               Gi3/0/4   N/A

<output truncated>
```

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.

show parser macro

Use the **show parser macro** user EXEC command to display the parameters for all configured macros or for one macro on the switch.

show parser macro [{**brief** | **description** [**interface** *interface-id*] | **name** *macro-name*}] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

brief	(Optional) Display the name of each macro.
description [**interface** *interface-id*]	(Optional) Display all macro descriptions or the description of a specific interface.
name *macro-name*	(Optional) Display information about a single macro identified by the macro name.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 a partial output example from the **show parser macro** 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
Total number of macros = 6
--------------------------------------------------------------
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
errdisable recovery cause link-flap
errdisable recovery interval 60

<output truncated>

--------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

<output truncated>

--------------------------------------------------------------
Macro name : cisco-phone
Macro type : default interface
# Cisco IP phone + desktop template
# macro keywords $AVID $VVID
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

<output truncated>

--------------------------------------------------------------
Macro name : cisco-switch
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Do not apply to EtherChannel/Port Group
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID

<output truncated>

--------------------------------------------------------------
Macro name : cisco-router
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID

<output truncated>

--------------------------------------------------------------
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

--------------------------------------------------------------
```

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
    default global   : cisco-global
    default interface: cisco-desktop
    default interface: cisco-phone
    default interface: cisco-switch
    default interface: cisco-router
    customizable     : snmp
```

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)
--------------------------------------------------------------
Gi1/0/1        standard-switch10
Gi1/0/2       this is test macro
--------------------------------------------------------------
```

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

```
Switch# show parser macro description interface gigabitethernet1/0/2
Interface    Macro Description
--------------------------------------------------------------
Gi1/0/2      this is test macro
--------------------------------------------------------------
```

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show running-config	Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command.

show policy-map

Use the **show policy-map** user EXEC command to display quality of service (QoS) policy maps, which define classification criteria for incoming traffic. Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

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

Syntax Description

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

Note Though visible in the command-line help string, the **control-plane** and **interface** keywords are not supported, and the statistics shown in the display should be ignored.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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
policy-map	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

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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)
-------------------------------------------------------------------------------
     Gi1/0/1         1             0             0            Shutdown
-------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

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

```
Switch# show port-security interface gigabitethernet1/0/1
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

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

```
Switch# show port-security address

Secure Mac Address Table
-------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi1/0/2     1
-------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

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

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

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

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

Related Commands

Command	Description
clear port-security	Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface.
switchport port-security	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

show sdm prefer

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

show sdm prefer [**access** | **default** | **dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} | **routing** | **vlan**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

access	(Optional) Display the template that maximizes system resources for ACLs.
default	(Optional) Display the template that balances system resources among features.
dual-ipv4-and-ipv6 {**default** | **routing** | **vlan**)	(Optional) Display the dual templates that support both IPv4 and IPv6. • **default**—Display the default dual template configuration. • **routing**—Display the routing dual template configuration. • **vlan**—Display the VLAN dual template configuration.
routing	(Optional) Display the template that maximizes system resources for routing.
vlan	(Optional) Display the template that maximizes system resources for Layer 2 VLANs.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

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** command, which displays the template in use:

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

  number of unicast mac addresses:             12K
  number of igmp groups + multicast routes:    1K
  number of unicast routes:                    0
  number of qos aces:                          0.5K
  number of security aces:                     1K
```

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

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

  number of unicast mac addresses:             6K
  number of igmp groups + multicast routes:    1K
  number of unicast routes:                    8K
    number of directly connected hosts:        6K
    number of indirect routes:                 2K
  number of policy based routing aces:         0
  number of qos aces:                          0.5K
  number of security aces:                     1K
```

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

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

  number of unicast mac addresses:             3K
  number of igmp groups + multicast routes:    1K
  number of unicast routes:                    11K
    number of directly connected hosts:        3K
    number of indirect routes:                 8K
  number of policy based routing aces:         0.5K
  number of qos aces:                          0.5K
  number of security aces:                     1K
```

This is an example of output from the **show sdm prefer dual-ipv4-and-ipv6 vlan** command:

```
Switch# show sdm prefer dual-ipv4-and-ipv6 vlan
 The current template is "desktop IPv4 and IPv6 vlan" template.
 The selected template optimizes the resources in  the switch to support this level of
 features for 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                 8K
  number of IPv4 IGMP groups:                      1K
  number of IPv4 multicast routes:                 0
  number of IPv4 unicast routes:                   0
  number of IPv6 multicast groups:                 1K
  number of directly-connected IPv6 addresses:     0
  number of indirect IPv6 unicast routes:          0
  number of IPv4 policy based routing aces:        0
  number of IPv4/MAC qos aces:                     0.5K
  number of IPv4/MAC security aces:                1K
  number of IPv6 policy based routing aces:        0
  number of IPv6 qos aces:                         0.5K
  number of IPv6 security aces:                    0.5K
```

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

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

  number of unicast mac addresses:                 12K
  number of IPv4 IGMP groups:                      1K
  number of IPv4 multicast routes:                 0
  number of IPv4 unicast routes:                   0
  number of IPv4 policy based routing aces:        0
  number of IPv4/MAC qos aces:                     0.5K
  number of IPv4/MAC security aces:                1K
```

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

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

  number of unicast mac addresses:           3K
  number of igmp groups + multicast routes:  1K
  number of unicast routes:                  11K
    number of directly connected hosts:      3K
    number of indirect routes:               8K
  number of qos aces:                        0.5K
  number of security aces:                   1K

 On next reload, template will be "desktop vlan" template.
```

Related Commands

Command	Description
sdm prefer	Sets the SDM template to maximize resources for routing or VLANs or to the default template, to select a dual IPv4 and IPv6 template, or to select the desktop templates.

show setup express

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

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

Syntax Description

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

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Examples

This is an example of output from the **show setup express co**mmand:

```
Switch# show setup express
express setup mode is active
```

Related Commands

Command	Description
setup express	Enables Express Setup mode.

show spanning-tree

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

show spanning-tree [*bridge-group* | **active** [**detail**] | **backbonefast** | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **mst** | **pathcost method** | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*] [**|** {**begin** | **exclude** | **include**} *expression*]

show spanning-tree *bridge-group* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree vlan *vlan-id* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree mst [**configuration** [digest]] | [*instance-id* [**detail** | **interface** *interface-id* [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

bridge-group	(Optional) Specify the bridge group number. The range is 1 to 255.
active [**detail**]	(Optional) Display spanning-tree information only on active interfaces (available only in privileged EXEC mode).
backbonefast	(Optional) Display spanning-tree BackboneFast status.
blockedports	(Optional) Display blocked port information (available only in privileged EXEC mode).
bridge [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display status and configuration of this switch (optional keywords available only in privileged EXEC mode).
detail [**active**]	(Optional) Display a detailed summary of interface information (**active** keyword available only in privileged EXEC mode).
inconsistentports	(Optional) Display inconsistent port information (available only in privileged EXEC mode).
interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**]	(Optional) Display spanning-tree information for the specified interface (all options except **portfast** and **state** available only in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.

mst [**configuration** [**digest**]] [*instance-id* [**detail** | **interface** *interface-id* [**detail**]]	(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode). The keywords have these meanings: • **digest**—(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). The terminology was updated for the implementation of the IEEE standard, and the *txholdcoun*t field was added. The new master role appears for boundary ports. The word *pre-standard* or *Pre-STD* appears when an IEEE standard bridge sends prestandard BPDUs on a port. The word *pre-standard (config)* or *Pre-STD-Cf* appears when a port has been configured to transmit prestandard BPDUs and no prestandard BPDU has been received on that port. The word *pre-standard (rcvd)* or *Pre-STD-Rx* appears when a prestandard BPDU has been received on a port that has not been configured to transmit prestandard BPDUs. A *dispute* flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated. • *instance-id*—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. • **interface** *interface-id*—(Optional) Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48. • **detail**—(Optional) Display detailed information for the instance or interface.
pathcost method	(Optional) Display the default path cost method (available only in privileged EXEC mode).
root [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]	(Optional) Display root switch status and configuration (all keywords available only in privileged EXEC mode).
summary [**totals**]	(Optional) Display a summary of port states or the total lines of the spanning-tree state section. The words *IEEE Standard* identify the MST version running on a switch.
uplinkfast	(Optional) Display spanning-tree UplinkFast status.
vlan *vlan-id* [**active** [**detail**] | **backbonefast** | **blockedports** | **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display spanning-tree information for the specified VLAN (some keywords available only in privileged EXEC mode). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 (GigabitEthernet2/0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

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

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

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

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 24 (GigabitEthernet2/0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled
```

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

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

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

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is enabled
BackboneFast         is enabled
Pathcost method used is short

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

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

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

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

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

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

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

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

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

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

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

Related Commands

Command	Description
clear spanning-tree counters	Clears the spanning-tree counters.
clear spanning-tree detected-protocols	Restarts the protocol migration process.
spanning-tree backbonefast	Enables the BackboneFast feature.
spanning-tree bpdufilter	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree extend system-id	Enables the extended system ID feature.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree link-type	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
spanning-tree loopguard default	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
spanning-tree mst configuration	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in an MST region before the BPDU is discarded and the information held for an interface is aged.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.
spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
spanning-tree vlan	Configures spanning tree on a per-VLAN basis.

show storm-control

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

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

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

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

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 a partial output from the **show storm-control** command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch> show storm-control
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi1/0/1      Forwarding     20 pps      10 pps     5 pps
Gi1/0/2      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 1/0/1
Interface    Filter State   Upper        Lower       Current
---------    -------------  ----------   ---------   ---------
Gi1/0/1      Forwarding     20 pps       10 pps      5 pps
```

Table 2-31 describes the fields in the **show storm-control** display.

Table 2-31 show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: • Blocking—Storm control is enabled, and a storm has occurred. • Forwarding—Storm control is enabled, and no storms have occurred. • Inactive—Storm control is disabled.
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
storm-control	Sets the broadcast, multicast, or unicast storm control levels for the switch.

show switch

Use the **show switch** user EXEC command to display information related to the stack member or the switch stack.

show switch [*stack-member-number* | **chassis-mgmt** | **detail** | **neighbors** | **stack-ports** | **stack-ring activity** [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Note This command is supported only on the Catalyst Switch Module 3110.

Syntax Description

stack-member-number	(Optional) Display information for the specified stack member. The range is 1 to 9.
chassis-mgmt	(Optional) Display information about the enclosures in which the stack members are installed.
detail	(Optional) Display detailed information about the stack ring.
neighbors	(Optional) Display the neighbors for the entire switch stack.
stack-ports	(Optional) Display port information for the entire switch stack.
stack-ring activity [**detail**]	(Optional) Display the number of frames per stack member that are sent to the stack ring. Use the **detail** keyword to display the ASIC, the receive queues, and the number of frames per stack member that are sent to the stack ring.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

These are the states displayed from this command:

- Waiting—The state when a switch is booting up and waiting for communication from other switches in the stack. The switch has not yet determined whether it is a stack master or not.

  Stack members not participating in a stack master election remain in the waiting state until the stack master is elected and ready.

- Initializing—The state when a switch has determined whether it is the stack master or not. If the switch is not the stack master, it is receiving its system- and interface-level configuration from the stack master and loading it.
- Ready—The state when the stack member has completed loading the system- and interface-level configuration and is ready to forward traffic.
- Master Re-Init—The state immediately after a stack master re-election and a different stack member is elected stack master. The new stack master is re-initializing its configuration. This state applies only to the new stack master.
- Ver Mismatch—The state of a switch in version mismatch (VM) mode. VM mode is when a switch joining the switch stack has a different stack protocol minor version number than the stack master.
- SDM Mismatch—The state of a switch in Switch Database Management (SDM) mismatch mode. SDM mismatch is when a stack member does not support the SDM template running on the stack master.
- Provisioned—The state of a preconfigured switch before it becomes an active member of a switch stack, or the state of a stack member after it has left the switch stack. The MAC address and the priority number in the display are always 0 for the provisioned switch.

A typical state transition for a stack member (including a stack master) booting up is Waiting -> Initializing -> Ready.

A typical state transition for a stack member becoming a stack master after a stack master election is Ready -> Master Re-Init -> Ready.

A typical state transition for a stack member in version mismatch (VM) mode is Waiting -> Ver Mismatch.

You can use the **show switch** command to identify whether the provisioned switch exists in the switch stack. The **show running-config** and the **show startup-config** privileged EXEC commands do not provide this information.

Examples

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

```
Switch> show switch
Switch/Stack Mac Address : 001b.540c.5d00
                                             H/W   Current
Switch#  Role   Mac Address     Priority Version  State
----------------------------------------------------------
*1       Master 001b.540c.5d00     10     1       Ready
 2       Member 0016.46ff.df00     1      1       Ready
```

This example shows output from the **show switch chassis-mgmt** command:

```
Switch#  Role    Slot#  Chassis ID
-------  ------  -----  --------------------------------
*1       Master  4      BEEF 1234 5678 9900 6969 6969 0123 DEAD

 2       Member  4      BEEB 9876 5432 1099 4646 3318 1221 BEEB
```

Related Commands

Command	Description
reload	Reloads the stack member and puts a configuration change into effect.
remote command	Monitors all or specified stack members.
session	Accesses a specific stack member.
switch priority	Changes the stack member priority value.
switch provision	Provisions a new switch before it joins the switch stack.
switch renumber	Changes the stack member number.

show system mtu

Use the **show system mtu** privileged EXEC command to display the global maximum transmission unit (MTU) or maximum packet size set for the switch.

show system mtu [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

Usage Guidelines

If you have used the **system mtu** or **system mtu jumbo** global configuration command to change the MTU setting, the new setting does not take effect until you reset the switch.

For information about the MTU values and the stack configurations that affect the MTU values, see the **system mtu** command.

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

Examples

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

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
On next reload, System Jumbo MTU will be 9198 bytes
Routing MTU size is 1500 bytes
```

Related Commands

Command	Description
system mtu	Sets the MTU size for the Gigabit Ethernet, 10-Gigabit Ethernet, or routed ports.

show udld

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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.

```
Switch> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
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: Gi2/0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi2/0/2
    Message interval: 5
    CDP Device name: Switch-A
```

Table 2-32 describes the fields in this display.

Table 2-32 show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state 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).

Related Commands

Command	Description
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again.

show version

Use the **show version** user EXEC command to display version information for the hardware and firmware and software license information only for the Catalyst Switch Module 3110.

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 version** command that shows the software licenses installed on the Catalyst Switch Module 3110:

Note Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

```
Switch> show version
Cisco IOS Software, CBS31X0 Software (CBS31X0-UNIVERSAL-M), Version 12.2(40)EX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 05-Oct-07 01:05 by myl
Image text-base: 0x00003000, data-base: 0x02000000

ROM: Bootstrap program is CBS31X0 boot loader
BOOTLDR: CBS31X0 Boot Loader (C31X0-HBOOT-M) Version 12.2(40r)EX, RELEASE SOFTWARE (fc1)
]

Switch uptime is 4 days, 19 hours, 17 minutes
System returned to ROM by power-on
System image file is "flash:cbs31x0-universal-mz.122-40.EX.bin"

License Level: ipbase   Type: Permanent
Next reboot license Level: ipbase

cisco WS-CBS31230X-S (PowerPC405) processor with 245760K/16376K bytes of memory.
Processor board ID FHH1128P00F
```

```
Last reset from power-on
Target IOS Version 12.2(40)EX
1 Virtual Ethernet interface
1 FastEthernet interface
52 Gigabit Ethernet interfaces
4 Ten Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:1B:54:0C:5D:00
Motherboard assembly number     : 73-10920-04
Motherboard serial number       : FHH11270015
Motherboard revision number     : 04
Model number                    : WS-CBS3110X-S
System serial number            : FHH1128P00F
Hardware Board Revision Number  : 0x00


Switch Ports Model              SW Version             SW Image
------ ----- -----              ----------             ----------
*    1 28    WS-CBS3110X-S      12.2(40)EX           CBS31X0-UNIVERSAL-M
     2 28    WS-CBS3110X-S      12.2(40)EX           CBS31X0-UNIVERSAL-M

Switch 02
---------
Switch Uptime                   : 4 days, 19 hours, 18 minutes
Base ethernet MAC Address       : 00:16:46:FF:DF:00
Motherboard assembly number     : 73-11920-03
Motherboard serial number       : FHH1111004R
Motherboard revision number     : 01
Model number                    : WS-CBS3110X-S
System serial number            : FSJC0712722
License Level                   : advipservices
License Type                    : Permanent
Next reboot licensing Level     : advipservices


Configuration register is 0xF
```

show vlan

Use the **show vlan** user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

show vlan [**brief** | **dot1q tag native** | **id** *vlan-id* | **internal usage** | **mtu** | **name** *vlan-name* | **private-vlan** [**type**] | **remote-span** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

brief	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
dot1q tag native	(Optional) Display the IEEE 802.1Q native VLAN tagging status.
id *vlan-id*	(Optional) Display information about a single VLAN identified by VLAN ID number. For *vlan-id*, the range is 1 to 4094.
internal usage	(Optional) Display 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 **vlan** global configuration command until you remove them from internal use.
mtu	(Optional) Display a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name *vlan-name*	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
private-vlan	(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 Catalyst Switch Module 3110 is running the IP services feature set.
type	(Optional) Display only private VLAN ID and type.
remote-span	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Display VLAN summary information.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	This command was introduced.

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 2-33 describes the fields in the display.

```
Switch> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14
1    default                          active    Gi2/0/1, Gi2/0/2, Gi2/0/3, Gi2/0/4
                                                Gi2/0/5, Gi2/0/6, Gi2/0/7, Gi2/0/8
                                                Gi2/0/9, Gi2/0/10, Gi2/0/11, Gi2/0/12
                                                Gi2/0/13, Gi2/0/14
<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  Gi1/0/1,Gi3/0/1
20      30     community Gi1/0/1, Gi3/0/1
20      35     community Gi1/0/1, Gi3/0/1

<output truncated>
```

Table 2-33 show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.
Primary/Secondary/ Type/Ports	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          Gi3/0/3
10      502       community         Gi2/0/11
10      503       non-operational3      -
20       25       isolated          Gi1/0/13, Gi1/0/1, Gi2/0/13,
                                    Gi3/0/13, Gi3/0/14, Gi3/0/1
20       30       community         Gi1/0/13, Gi1/0/1, Gi2/0/13,
                                    Gi3/0/14, Gi3/0/1
```

```
20       35       community         Gi1/0/13, Gi1/0/1,
                                    Gi2/0/13, Gi3/0/14, Gi3/0/1
20       55       non-operational
2000   2500       isolated          Gi1/0/5, Gi1/0/10, Gi2/0/5, Gi2/0/10
```

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    Gi1/0/7, Gi1/0/8
2    VLAN0200                         active    Gi2/0/1, Gi2/0/2

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 Gigabit Ethernet routed ports 7 and 8 on stack member 1. If you want to use one of these VLAN IDs, you must first shut down the routed port, which releases the internal VLAN, and then create the extended-range VLAN. When you start up the routed port, another internal VLAN number is assigned to it.

```
Switch> show vlan internal usage
VLAN Usage
---- -------------
1025 GigabitEthernet1/0/7
1026 GigabitEthernet1/0/8
```

Related Commands

Command	Description
private-vlan	Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs.
switchport mode	Configures the VLAN membership mode of a port.
vlan (global configuration)	Enables VLAN configuration mode where you can configure VLANs 1 to 4094.
vlan (VLAN configuration)	Configures VLAN characteristics in the VLAN database. Only available for normal-range VLANs (VLAN IDs 1 to 1005). Do not enter leading zeros.

show vlan access-map

Use the **show vlan access-map** privileged EXEC command to display information about a particular VLAN access map or for all VLAN access maps.

show vlan access-map [*mapname*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

show vlan filter

Use the **show vlan filter** privileged EXEC command to display information about all VLAN filters or about a particular VLAN or VLAN access map.

show vlan filter [**access-map** *name* | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(40)EX2	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
show vlan access-map	Displays information about a particular VLAN access map or for all VLAN access maps.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

show vmps

Use the **show vmps** user EXEC command without keywords to display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers, or use the **statistics** keyword to display client-side statistics.

show vmps [**statistics**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 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 2-34 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 2-34 show vmps statistics Field Descriptions

Field	Description
VQP Queries	Number of queries sent by the client to the VMPS.
VQP Responses	Number of responses sent to the client from the VMPS.
VMPS Changes	Number of times that the VMPS changed from one server to another.
VQP Shutdowns	Number of times the VMPS sent a response to shut down the port. The client disables the port and removes all dynamic addresses on this port from the address table. You must administratively re-enable the port to restore connectivity.
VQP Denied	Number of times the VMPS denied the client request for security reasons. When the VMPS response denies an address, no frame is forwarded to or from the workstation with that address (broadcast or multicast frames are delivered to the workstation if the port has been assigned to a VLAN). The client keeps the denied address in the address table as a blocked address to prevent more queries from being sent to the VMPS for each new packet received from this workstation. The client ages the address if no new packets are received from this workstation on this port within the aging time period.
VQP Wrong Domain	Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. This response means that the server and the client have not been configured with the same VTP management domain.
VQP Wrong Version	Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. The VLAN assignment of the port is not changed. The switches send only VMPS Version 1 requests.
VQP Insufficient Resource	Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached.

Related Commands

Command	Description
clear vmps statistics	Clears the statistics maintained by the VQP client.
vmps reconfirm (privileged EXEC)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.
vmps retry	Configures the per-server retry count for the VQP client.
vmps server	Configures the primary VMPS and up to three secondary servers.

show vtp

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(40)EX2	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 vtp counters** command.

```
Switch> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/0/47           0                0                0
Gi1/0/48           0                0                0
Gi2/0/1            0                0                0
Gi3/0/2            0                0                0
```

Table 2-35 describes each field in the display.

Table 2-35 show vtp counters Field Descriptions

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

Table 2-35 show vtp counters Field Descriptions (continued)

Field	Description
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP Version 1 frame. These errors mean that at least one neighboring switch is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. Table 2-36 describes each field in the display.

```
Switch> show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 45
VTP Operating Mode              : Transparent
VTP Domain Name                 : shared_testbed1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Enabled
MD5 digest                      : 0x3A 0x29 0x86 0x39 0xB4 0x5D 0x58 0xD7
```

Table 2-36 show vtp status Field Descriptions

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

Table 2-36 show vtp status Field Descriptions (continued)

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

Related Commands

Command	Description
clear vtp counters	Clears the VTP and pruning counters.
vtp (global configuration)	Configures the VTP filename, interface name, domain name, and mode.
vtp (VLAN configuration)	Configures the VTP domain name, password, pruning, and mode.