rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics, which include usage statistics about broadcast and multicast packets, and error statistics about cyclic redundancy check (CRC) alignment errors and collisions. Use the **no** form of this command to return to the default setting.

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

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

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(25)EX	This command was introduced.

Usage Guidelines

The RMON statistics collection command is based on hardware counters. If the port is a user network interface (UNI), you must use the **no shutdown** interface configuration command to enable it before using the **rmon collection stats** command. UNIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

Examples

This example shows how to collect RMON statistics for the owner *root*:

```
Switch(config)# interface gigabitethernet0/1
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 to configure the template used in Switch Database Management (SDM) resource allocation. If the switch is running the metro IP access image, you can use a template to balance resources between Layer 2 and Layer 3 functionality, or you can maximize system usage to support only Layer 2 features in hardware. Use the **no** form of this command to return to the default template.

sdm prefer {**default | layer-2**}

no sdm prefer

Syntax Description

default	Give balance to all functions.
layer-2	Maximizes system resources for Layer 2 functionality and does not support routing in hardware.

Defaults

The default template provides a balance to all features.

Note On switches that are running the metro base image or the metro access image, only the layer-2 template is supported.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12.2(25)SE	The number of unicast MAC addresses supported by the default template was increased to 5K.

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.

The default templates balances the use of system resources. Do not use the default template if you do not have routing enabled on your switch. Using the balanced template prevents Layer 2 features from using the memory allocated to unicast routing in the default template.

Do not use the layer-2 template if the switch is routing packets. The layer-2 template does not support routing and forces any routing to be done through software. This overloads the CPU and severely degrades routing performance.

Table 2-4 lists the approximate number of each resource supported in each of the templates for a switch running the metro IP access image. The values in the template are based on eight routed interfaces and approximately 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 2-4 Approximate Number of Feature Resources Allowed by Each Template

Resource	Layer-2	Default
Unicast MAC addresses	8 K	5 K
IPv4 IGMP groups and multicast routes (default only)	–	1 K
IP v4 IGMP groups (layer-2 template only)	1 K	–
IPv4 multicast routes (layer-2 template only)	0	–
IPv4 IGMP groups and multicast routes	1 K	–
IPv4 unicast routes	0	9 K
Directly connected IPv4 hosts	–	5 K
Indirect IPv4 routes	–	4 K
IPv4 policy-based routing access control entries (ACEs)	0	512
IPv4 or MAC quality of service (QoS) ACEs	512	512
IPv4 or MAC security ACEs	1 K	1 K

Examples

This example shows how to configure the layer-2 template on a switch:

```
Switch(config)# sdm prefer layer-2
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 the approximate resource allocation per feature.

service instance

Use the **service instance** interface configuration command to configure an Ethernet service instance on the interface and to enter Ethernet service configuration mode. Use the **no** form of this command to delete the service instance.

service instance *id* **ethernet** [*evc-id*]

no service instance *id*

This command is available only if your switch is running the metro IP access or metro access image.

Syntax Description

id	Define a service instance identifier, a per-interface service identifier that does not map to a VLAN. The range is 1 to 4294967295.
ethernet	Identify the service instance as an Ethernet instance.
evc-id	(Optional) Attach an Ethernet virtual connection (EVC) to the service instance.

Defaults

No Ethernet service instances are defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SEG	This command was introduced.

Usage Guidelines

After you enter the **service instance** *id* **ethernet** command, the switch enters Ethernet service configuration mode, and these configuration commands are available:

- **default**: sets the service instance to its default state.
- **ethernet lmi ce-vlan map**: configures Ethernet Local Management Interface (LMI) parameters. See the **ethernet lmi ce-vlan map** command.
- **exit**: exits EVC configuration mode and returns to global configuration mode.
- **no**: negates a command or returns a command to its default setting.

Examples

This example shows how to define an Ethernet service instance and to enter Ethernet service configuration mode for EVC *test*:

```
Switch(config-if)# service instance 333 ethernet test
Switch(config-if-srv)#
```

Related Commands

Command	Description
show ethernet service instance	Displays information about configured Ethernet service instances.

service password-recovery

Use the **service password-recovery** global configuration command to enable the password-recovery mechanism (the default). This mechanism allows an end user with physical access to the switch to press the break key on the console terminal to 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(25)EX	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. This provides configuration file security by ensuring that only authenticated and authorized users have access to the configuration file and prevents users from accessing the configuration file by using the password recovery process.

The password recovery procedure requires using a break key. After the switch performs power-on self test (POST), the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

```
***** The system will autoboot in 5 seconds *****

Send a break key to prevent autobooting.
```

You must enter the break key on the console terminal within 5 seconds of receiving the message that the system will autoboot. A user with physical access to the switch presses the break key on the console terminal within 5 seconds of receiving the message that flash memory is initializing. The System LED flashes green until the **break key** is accepted. After the **break key** is accepted, the System LED turns off until after the switch boots.

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 **break key** 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 configuration 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 configuration file on the switch.

You can enter the **show version** privileged EXEC command to determine if password recovery is enabled or disabled.

Examples

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

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

Related Commands

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

service-policy (interface configuration)

Use the **service-policy** interface configuration command to apply a policy map defined by the **policy-map** command to the incoming or outgoing traffic of a physical port. Use the **no** form of this command to remove the policy map and port association.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input	Apply the policy map to the input of a physical port.
output	Apply the policy map to the output of a physical port.
policy-map-name	The specified policy map to be applied.

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

Defaults

No policy maps are attached to the port.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.

Usage Guidelines

Only one input policy map and one output policy map can be attached to an interface.

Beginning with Cisco IOS Release 12.2(35)SE, you can attach an output policy map to each interface on the switch. However, the switch supports a limit of three unique queue-limit configurations across all output policy maps at any time. Multiple policy maps can share the same queue-limit configuration.If you try to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

You can attach input or output policy maps to a Fast Ethernet or Gigabit Ethernet port. You cannot attach policy maps to switch virtual interfaces (SVIs) and EtherChannel interfaces.

Examples

This example shows how to apply *plcmap1* as an output policy map:

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

This example shows how to remove *plcmap2* from the port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no service-policy output plcmap2
```

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

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.
show policy-map interface [*interface-id*]	Displays policy maps configured on the specified interface or on all interfaces.
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.

service-policy (policy-map class configuration)

Use the **service-policy** policy-map class configuration command to configure a quality of service (Q0S) service policy for an input or output policy map or a per-port, per-VLAN policy map. Use the **no** form of this command to disable a service policy as a QoS policy within a policy map.

service-policy *policy-map-name*

no service-policy *policy-map-name*

Syntax Description

policy-map-name	Name of the service policy map (created by using the **policy-map** global configuration command) to be used in a QoS hierarchical service policy.

Defaults

No service policies are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12.2(25)SEG	Support was added for the ability to use this command to assign a child QoS policy to a parent input policy defined by classifying based on VLAN ID (supported with only the metro IP access or metro access image). See "Usage Guidelines."

Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, if the switch is running the metro IP access or metro access image, you can use the **service-policy input** command to assign a child QoS policy to a parent input policy defined with a classification based on VLAN IDs. This allows you to create a hierarchical policy for per-port, per-VLAN QoS.

You attach a service policy created in policy-map class configuration to a parent output policy map. This creates hierarchical policy mapping. Use the **service-policy** *policy-map-name* policy-map class configuration command to enter a second-level (child) policy map.

For an input policy map, when you configure classes with classification based on VLAN IDs by using the **match vlan** class-map configuration command, you can use **service-policy** policy-map class configuration command to associate a child QoS policy with that class. This provides the ability to apply independent QoS policies based on the VLAN IDs of the incoming traffic on the port. The per-port, per-vlan ingress QoS feature is supported only using a 2-level hierarchical input policymap, where the parent level defines the VLAN-based classification and the child level defines the QoS policy to be applied to the corresponding VLAN or VLANs. You can configure the child policy with all actions that are available for input policy maps, specifically policing and marking.

Note Per-port, per-VLAN QoS is supported only when the switch is running the metro IP access or metro access image.

For an output policy map, when **shape average** is also configured on the class **class-default**, you can configure hierarchical policy maps by attaching a single **service-policy** policy-map class command to the class **class-default**. This policy map specifies the service policy for the port-shaped traffic on the port and is the parent policy map. You can configure the child policy with class-based queuing actions by using the **queue-limit** policy map class command and with scheduling actions (by using the **bandwidth**, **shape average**, or **priority** command).

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 define the service policy and to attach it to a parent policy map to set the maximum bandwidth (shape) for an output queue at 90000000 bits per second:

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

In this example, the class maps in the child-level policy map specify matching criteria for voice and video traffic, and the child policy map sets the action for input policing each type of traffic. The parent-level policy map specifies the VLANs to which the child policy maps are applied on the specified port.

```
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```

Note You can also enter the match criteria as **match vlan 100 200 300** with the same result.

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# set ip precedence 4
Switch(config-pmap-c)# exit

Switch(config)# policy-map parent-customer-1
Switch(config-pmap)# class customer-1-vlan
Switch(config-pmap-c)# service-policy ingress-policy-1
Switch(config-pmap-c)# 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 for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

set cos

Use the **set cos** policy-map class configuration command to set a Layer 2 class of service (CoS) value in the packet. Use the **no** form of this command to remove traffic marking.

set cos {*cos_value* | *from-field* [**table** *table-map-name*]}

no set cos {*cos_value* | *from-field* [**table** *table-map-name*]}

Syntax Description

cos_value	Enter an IEEE 802.1Q class of service/user priority value with which to classify traffic. The range is from 0 to 7.
from-field	Specific a packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the *map-from* packet-marking category. These options are supported: • **cos**—CoS value • **dscp**—Differentiated Services Code Point (DSCP) value. • **precedence**—IP-precedence value
table	(Optional) Used in conjunction with the *from-field* keyword. Indicates that the values set in a specified table map are used to set the CoS value
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12-2(25)SEG	Support was added to set multiple marking actions and to use table maps for enhanced packet marking. See “Usage Guidelines.”

Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure **set cos** with all other marking actions, specifically **set dscp**, **set precedence**, and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

Use the **set cos** command if you want to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information including a CoS value marking.

You can use the **match cos** class-map configuration command and the **set cos** policy-map class configuration command together to allow switches to interoperate and provide quality of service (QoS) based on the CoS markings. You can also configure Layer 2 to Layer 3 mapping by matching on the CoS value because switches can already match and set CoS values.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the CoS value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name,* the default action is to copy the value associated with the *from-field* category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence value is copied and used as the CoS value. If you enter the **set cos dscp** command, the DSCP value is copied and used as the CoS value.

Examples

This example shows how to set all FTP traffic to cos 3:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
```

This example shows how to assign a DSCP to CoS table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos dscp table dscp-cos-tablemap
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 for the specified class-map name.
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.

set dscp

Use the **set** [**ip**] **dscp** policy-map class configuration command to mark IPv4 traffic by setting a Differentiated Services Code Point (DSCP) value in the type of service (ToS) byte of the packet. Use the **no** form of this command to remove traffic marking.

set [**ip**] **dscp** {*dscp_value* |*from-field* [**table** *table-map-name*]}

no set [**ip**] **dscp** {*dscp_value* | *from-field* [**table** *table-map-name*]}

Note Entering **ip dscp** is the same as entering **dscp**.

Syntax Description

dscp-value	Enter a DSCP value with which to classify traffic. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
from-field	Specific a packet-marking category to be used to set the DSCP value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the *map-from* packet-marking category. These options are supported: • **cos**—class of service (CoS) value • **dscp**—DSCP value. • **precedence**—IP-precedence value
table	(Optional) Used in conjunction with the *from-field* keyword. Indicates that the values set in a specified table map are used to set the DSCP value
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12-2(25)SEG	Support was added to set multiple marking actions and to use table maps for enhanced packet marking. See “Usage Guidelines.”

Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure **set dscp** with other marking actions, specifically **set cos** and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

You cannot use the **set dscp** command with the **set precedence** command to mark the same packet. DSCP values and IP precedence values are mutually exclusive. A packet can have one value of the other, but not both.

After DSCP bits are set, other quality of service (QoS) features can then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the DSCP value at the edge of the network (or administrative domain) and data is then queued according to the precedence. Class-based weighted fair queuing (CBWFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Tail Drop (WTD) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Instead of using numeric values, you can also specify the *dscp-value* by using the reserved keywords **EF**, **AF11**, and **AF12**.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the DSCP value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name,* the default action is to copy the value associated with the *from-field* category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value is copied and used as the DSCP value.

Examples

This example shows how to set all FTP traffic to DSCP 10:

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

This example shows how to assign a CoS to DSCP table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp cos table cos-dscp-tablemap
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 for the specified class-map name.
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.

set precedence

Use the **set** [**ip**] **precedence** policy-map class configuration command to mark IPv4 traffic by setting an IP-precedence value in the packet. Use the **no** form of this command to remove traffic marking.

set [**ip**] **precedence** {*precedence_value* | *from-field* [**table** *table-map-name*]}

no set [**ip**] **precedence** {*precedence_value* | *from-field* [**table** *table-map-name*]}

Note Entering **ip precedence** is the same as entering **precedence**.

Syntax Description

precedence_value	Enter an IPv4 precedence value with which to classify traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
from-field	Specific a packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the *map-from* packet-marking category. These options are supported: • **cos**—class of service (CoS) value • **dscp**—Differentiated Services Code Point (DSCP) value. • **precedence**—IP-precedence value
table	(Optional) Used in conjunction with the *from-field* keyword. Indicates that the values set in a specified table map are used to set the precedence value
table-map-name	(Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12-2(25)SEG	Support was added to set multiple marking actions and to use table maps for enhanced packet marking. See “Usage Guidelines.”

Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure **set precedence** with other marking actions, specifically **set cos** and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

You cannot use the **set precedence** command with the **set dscp** command to mark the same packet. DSCP values and IP precedence values are mutually exclusive. A packet can have one value of the other, but not both.

After precedence bits are set, other quality of service (QoS) features can then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain) and data is then queued according to the precedence. Class-based weighted fair queuing (CBWFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Tail Drop (WTD) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Instead of using numeric values, you can also specify the *dscp-value* by using the reserved keywords **EF**, **AF11**, and **AF12**.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the precedence value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name,* the default action is to copy the value associated with the *from-field* category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value is copied and used as the precedence value.

Examples

This example shows how to give all FTP traffic an IP precedence value of 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set precedence 5
Switch(config-pmap-c)# exit
```

This example shows how to assign a CoS to precedence table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set precedence cos table cos-prec-tablemap
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 for the specified class-map name.
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.

set qos-group

Use the **set qos-group** policy-map class configuration command to set a a quality of service (QoS) group identifier that can be used later to classify packets. Use the **no** form of this command to remove the group identifier.

set qos-group *value*

no set qos-group *value*

Syntax Description

value	Set the QoS group value to use to classify traffic. The range is from 0 to 99.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12.2(25)SEG	The number of supported QoS groups was increased to 100. Support was added to set multiple marking actions and to use table maps for enhanced packet marking. See "Usage Guidelines."

Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure **set qos-group** with all other marking actions, specifically **set cos, set dscp**, and **set precedence**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

Use this command to associate a QoS group value with a traffic flow as it enters the switch, which can then be used in an output policy map to identify the flow.

A maximum of 100 QoS groups (0 through 99) is supported on the switch.

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 set all FTP traffic to QoS group 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set qos-group 5
Switch(config-pmap-c)# 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 for the specified class-map name.
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.

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(25)EX	This command was introduced.

Usage Guidelines

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

- IP address and network mask
- Password strategy for your environment

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

GigabitEthernet0/1         unassigned      YES unset  up                    up

GigabitEthernet0/2         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

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 GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
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.

shape average

Use the **shape average** policy-map class configuration command to configure class-based shaping by specifying the average traffic shaping rate. Use the command with the class **class-default** to set port shaping. Use the **no** form of this command to remove traffic shaping.

shape average *target bps*

no shape average *target bps*

Syntax Description

target bps	Target average bit rate in bits per second (bps). The range is from 64000 to 1000000000.

Defaults

No traffic shaping is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12.2(25)SEG	Support was added to configure traffic shaping in the **class-default** of an output policy map.

Usage Guidelines

You use the **shape average** policy-map class command to control output traffic. Shaping is not supported in input policy maps.

Traffic shaping limits the rate of transmission of data. Configuring traffic shaping for a user-defined class or **class-default** for class-based shaping sets the peak information rate (PIR) for that class. Configuring traffic shaping for the class **class-default** when it is the only class in the policy map that is attached to an interface sets the PIR for the interface (port shaping).

You cannot configure **shape average** in a class that includes priority queueing (configured with the **priority** policy-map class configuration command).

The **shape average** command uses a default queue limit for the class. You can change the queue limit by using the **queue-limit** policy-map class command, overriding the default that is set by the **shape average** command.

You cannot use the **bandwidth** policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ) and the **shape average** command to configure traffic shaping for the same class.

You can configure hierarchical policy maps by attaching the **service-policy** policy-map class command to the class **class-default** only when **shape average** is also configured on the class **class-default**.

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 configure traffic shaping for outgoing traffic on a Fast Ethernet port so that *outclass1*, *outclass2*, and *outclass3* get a maximum of 50, 20, and 10 Mbps of the buffer size. The class **class-default** gets the remaining bandwidth.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy out out-policy
```

This example shows how to configure port shaping by configuring a hierarchical policy map that shapes a port to 90 Mbps, allocated according to the *out-policy* policy map configured in the previous example.

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
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 for the specified class-map name.
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 policy-map interface [*interface-id*]	Displays policy maps configured on the specified interface or on all interfaces.

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(25)EX	This command was introduced.

Usage Guidelines

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

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
```

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(25)EX	This command was introduced.

Usage Guidelines

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

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*]

Note This command is available only if your switch is running the metro IP access or metro access image.

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(25)EX	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 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(25)EX	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. Table 2-5 describes each field in the display.

```
Switch# show boot
5d05h: %SYS-5-CONFIG_I: Configured from console by console
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : yes
HELPER path-list    :
Auto upgrade        : yes
```

Table 2-5 show boot Field Descriptions

Field	Description
BOOT path-list	Displays a semicolon separated list of executable files to try to load and execute when automatically booting. 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.

Table 2-5 show boot Field Descriptions (continued)

Field	Description
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 the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
Helper path-list	Displays a semicolon separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

Related Commands

Command	Description
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*]

Note TDR is supported only on the copper Ethernet 10/100 ports on the Cisco ME switch.

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(25)EX	This command was introduced.

Usage Guidelines

TDR is supported only on copper Ethernet 10/100 ports on the Cisco ME switch. It is not supported on small form-factor pluggable (SFP)-module 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 on a Cisco ME switch:

```
Switch# show cable-diagnostics tdr interface fastethernet0/1
TDR test last run on: March 01 18:14:44

Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Fa0/1     100M  Pair A     4    +/- 5  meters Pair A      Normal
                Pair B     4    +/- 5  meters Pair B      Normal
                Pair C     N/A                Pair C      N/A
                Pair D     N/A                Pair D      N/A
```

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

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

Field	Description
Interface	Interface on which TDR was run.
Speed	Speed of connection.
Local pair	Name of the pair of wires that TDR is testing on the local interface.
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 100 Mbps. • The cable is open. • The cable has a short.
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can 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.

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

```
Switch# show interface fastethernet0/1
fastethernet0/1 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 fastethernet0/1
% TDR test was never issued on fa0/1
```

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(25)EX	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 access-group	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(25)EX	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, 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(25)EX	This command was introduced.

Usage Guidelines

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

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

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 2-7 describes the *Transmit* fields, and Table 2-8 describes the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitethernet0/1
Transmit GigabitEthernet0/1            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 2-7 Transmit Field Descriptions

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

Table 2-7 Transmit Field Descriptions (continued)

Field	Description
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excessive collisions	The number of frames that could not be sent on an interface after 16 collisions occur.
Late collisions	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
VLAN discard frames	The number of frames dropped on an interface because the CFI[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 2-8 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 2-8 Receive Field Descriptions (continued)

Field	Description
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast bytes	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Alignment errors	The total number of frames received on an interface that have alignment errors.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
Oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size.
Undersize frames	The number of frames received on an interface that are smaller than 64 bytes.
Collision fragments	The number of collision fragments received on an interface.
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
Overrun frames	The total number of overrun frames received on an interface.
Pause frames	The number of pause frames received on an interface.
Symbol error frames	The number of frames received on an interface that have symbol errors.
Invalid frames, too large	The number of frames received that were larger than maximum allowed MTU[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 2-8 Receive Field Descriptions (continued)

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

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

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

```
Switch# show controllers ethernet-controller gigabitethernet0/2 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 port-asic configuration** command:

```
Switch# show controllers ethernet-controller port-asic configuration
================================================================================
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
==========================================================================
 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
=====================================================================================
 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 ternary content addressable memory (TCAM) in the system and for TCAM interface ASICs that are CAM controllers.

show controllers tcam

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)EX	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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Fa0/1            0                    0
Fa0/2            0                    0
Fa0/3            0                    0
Fa0/4            0                    0
Fa0/5            0                    0
Fa0/6            0                    0
Fa0/7            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 gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

Table 2-9 show controllers utilization Field Descriptions

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

Note This command is visible only when the switch is running the metro IP access or metro access image.

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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch> show dot1q-tunnel
dot1q-tunnel mode LAN Port(s)
------------------------------
Gi0/1
Gi0/2
Gi0/3
Gi0/6
Po2

Switch> show dot1q-tunnel interface gigabitethernet0/1
dot1q-tunnel mode LAN Port(s)
------------------------------
Gi0/1
```

Related Commands

Command	Description
show vlan dot1q tag native	Displays 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** privileged EXEC command to display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

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

Syntax Description

all	(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, module, and port number).
statistics interface *interface-id*	(Optional) Display IEEE 802.1x statistics for the specified port (including type, 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(25)EX	This command was introduced.

Usage Guidelines

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

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** and the **show dot1x all** privileged EXEC commands:

```
Switch# show dot1x
Sysauthcontrol                  = Enabled
Supplicant Allowed In Guest Vlan  = Disabled
Dot1x Protocol Version          = 1
Dot1x Oper Controlled Directions  = Both
Dot1x Admin Controlled Directions = Both

Switch# show dot1x all
Dot1x Info for interface GigabitEthernet0/1
----------------------------------------------------
```

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

Dot1x Info for interface GigabitEthernet0/2
----------------------------------------------------
PortStatus        = UNAUTHORIZED
MaxReq            = 2
HostMode          = Multi
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

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

```
Switch# show dot1x interface gigabitethernet0/1
Supplicant MAC 00d0.b71b.35de
   AuthSM State      = AUTHENTICATED
   BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

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

```
Switch# show dot1x statistics interface gigabitethernet0/1
PortStatistics Parameters for Dot1x
---------------------------------------
TxReqId = 15    TxReq = 0       TxTotal = 15
RxStart = 4     RxLogoff = 0    RxRespId = 1    RxResp = 1
RxInvalid = 0   RxLenErr = 0    RxTotal= 6
RxVersion = 1   LastRxSrcMac 00d0.b71b.35de
```

Table 2-10 show dot1x statistics Field Descriptions

Field	Description
TxReqId	Number of Extensible Authentication Protocol (EAP)-request/identity frames that have been sent.
TxReq	Number of EAP-request frames (other than request/identity frames) that have been sent.
TxTotal	Number of Extensible Authentication Protocol over LAN (EAPOL) frames of any type that have been sent.
RxStart	Number of valid EAPOL-start frames that have been received.
RxLogoff	Number of EAPOL-logoff frames that have been received.
RxRespId	Number of EAP-response/identity frames that have been received.
RxResp	Number of valid EAP-response frames (other than response/identity frames) that have been received.
RxInvalid	Number of EAPOL frames that have been received and have an unrecognized frame type.
RxLenError	Number of EAPOL frames that have been received in which the packet body length field is invalid.
RxTotal	Number of valid EAPOL frames of any type that have been received.
RxVersion	Number of received packets in the 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 configurable IEEE 802.1x parameters to their default values.

show env

Use the **show env** user EXEC command to display fan, temperature, redundant power system (RPS) availability, and power information for the switch.

show env {**all** | **fan** | **power** | **rps** | **temperature [status]**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display both fan and temperature environmental status.
fan	Display the switch fan status.
power	Display the switch power status.
rps	Display whether a Cisco RPS 300 Redundant Power System is connected to the switch. This keyword is not visible on all platforms; the Cisco ME switch does not support the RPS
temperature	Display the switch temperature status as OK or FAULTY.
status	(Optional) Show more detailed temperature status, including the temperature value, state (green, yellow, or red), and the yellow and red threshold values. **Note** Temperature status is supported only on the Cisco ME-3400-12CS and ME-3400-2CS switches.
| 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(25)EX	This command was introduced.
12.2(25)SEG1	The **status** keyword was added. The outputs were expanded to reflect the dual fans, dual power supplies, and temperature setting for the Cisco ME 3400G-12CS switches and temperature setting for the Cisco ME 3400-2 CS switch.

Usage Guidelines

On a Cisco ME 3400-12CS and ME 3400 2CS switches, you can use the **show env temperature status** 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 on this switch, the command output is the same as the **show env temperature status** command output.

You can use the **system env temperature threshold yellow** global configuration command to configure the yellow temperature threshold. If not configured, the yellow threshold defaults to 10 degrees Celsius below the red threshold.

For more information about the threshold levels, see the software configuration guide for this release.

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

Examples

Displays for the Cisco ME 3400G-12CS or ME 3400 2CS switch are different than those for other Cisco ME 3400 switches. This is an example of output from the **show env all** command for the Cisco ME 3400G-12CS switch:

```
Switch> show env all
FAN 1 is OK
FAN 2 is OK
TEMPERATURE is OK
Temperature Value: 31 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 56 Degree Celsius
Red Threshold    : 66 Degree Celsius
POWER SUPPLY 1 is OK
POWER SUPPLY 2 is Alarm disabled
```

This is an example of output from the **show env all** command for the Cisco ME 3400G-2CS switch:

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
Temperature Value: 37 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 45 Degree Celsius
Red Threshold : 55 Degree Celsius
POWER is OK
```

This is an example of output from the **show env all** command for other Cisco ME switches:

```
Switch# show env all
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

This is an example of output from the **show env fan** command for the Cisco ME 3400G-12CS switch:

```
Switch> show env fan
FAN 1 is OK
FAN 2 is OK
```

This is an example of output from the **show env fan** command for other Cisco ME switches:

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

This is an example of output from the **show env power** command for the Cisco ME 3400G-12CS switch:

```
Switch> show env power
POWER SUPPLY 1 is OK
POWER SUPPLY 2 is Alarm disabled
```

These are examples of output from the **show env temperature** command for the Cisco ME 3400G-12CS or ME-3400-2CS switch:

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

```
Switch> show env temperature status
Temperature Value: 31 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 56 Degree Celsius
Red Threshold    : 66 Degree Celsius
```

Related Commands

Command	Description
power-supply dual	Sets or suppresses alarms for the switch second power supply.
system env temperature threshold yellow	Configures the yellow temperature threshold.

show errdisable detect

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12.2(37)SE	The `Mode` column was added to the output display.

Usage Guidelines

The `Mode` column shows the shutdown mode that was configured for the error-disabled reason:

- port—The physical port is error disabled if a violation occurs.
- vlan—The virtual port is disabled if a violation occurs.
- port/vlan—Some ports are configured for physical port disable, and others are configured for virtual port disable. Enter the **show running config** privileged EXEC command to see the configuration for each port.

A displayed `gbic-invalid` error in the `Reason` column refers to an invalid small form-factor pluggable (SFP) interface.

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

Examples

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

```
Switch> show errdisable detect
ErrDisable Reason   Detection   Mode
-----------------   ---------   ----
arp-inspection      Enabled   port
bpduguard           Enabled   port
channel-misconfig   Enabled   port
community-limit     Enabled   port
dhcp-rate-limit     Enabled   port
dtp-flap            Enabled   port
gbic-invalid        Enabled   port
invalid-policy      Enabled   port
l2ptguard           Enabled   port
link-flap           Enabled   port
link-monitor-fail   Enabled   port
```

```
loopback            Enabled   port
lsgroup             Enabled   port
oam-remote-failur   Enabled   port
pagp-flap           Enabled   port
psecure-violation   Enabled   port/vlan
security-violatio   Enabled   port
sfp-config-mismat   Enabled   port
storm-control       Enabled   port
udld                Enabled   port
vmps                Enabled   port
```

Note Though visible in the output, the dtp-flap, ilpower, storm-control, and unicast-flood fields are not valid.

Related Commands

Command	Description
errdisable detect cause	Enables error-disable detection for a specific cause or all causes.
show errdisable flap-values	Displays error condition recognition information.
show errdisable recovery	Displays error-disable recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in an 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(25)EX	This command was introduced.

Usage Guidelines

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

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

Note Although visible in the output display, the switch does not support DTP.

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

Examples

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

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

Related Commands

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

show errdisable recovery

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)EX	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.

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

Examples

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

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
l2ptguard            Disabled
link-flap            Enabled
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)
---------    -----------------    --------------
Gi0/2        link-flap             279
```

Note Though visible in the output, the unicast-flood and DTP fields are 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(25)EX	This command was introduced.

Usage Guidelines

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

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

Note The switch must be running the metro IP access image to support Layer 3 ports.

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

Examples

This is an example of output from the **show 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: Gi0/1
------------

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
Gi0/1     SA      bndl      32768         0x0       0x1     0x0      0x3D

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

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

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

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

Ports in the Port-channel:

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

Time since last port bundled:    01d:20h:20m:20s    Gi0/2
```

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      Gi0/1(P)    Gi0/2(P)
```

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

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

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

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

Ports in the Port-channel:

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

Time since last port bundled:    01d:20h:24m:44s    Gi0/2
```

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 ethernet service evc

Use the **show ethernet service evc** privileged EXEC command to display information about Ethernet virtual connection (EVC) customer-service instances.

show ethernet service evc [**id** *evc-id* | **interface** *interface-id*] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

This command is available only if your switch is running the metro IP access or metro access image.

Syntax Description

id *evc-id*	(Optional) Display EVC information for the specified service. The EVC identifier can be a string of from 1 to 100 characters.
interface *interface-id*	(Optional) Display EVC information for the specified interface.
detail	(Optional) Display detailed information about EVC service or the specified EVC ID or 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

Privileged EXEC

Command History

Release	Modification
12.2(25)SEG	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 ethernet service evc** command:

```
Switch# show ethernet service evc
Identifier                      Type  Act-UNI-cnt Status
BLUE                            P-P       2       Active
PINK                            MP-MP     2       PartiallyActive
PURPLE                          P-P       2       Active
BROWN                           MP-MP     2       Active
GREEN                           P-P       3       Active
YELLOW                          MP-MP     2       PartiallyActive
BANANAS                         P-P       0       InActive
TEST2                           P-P       0       NotDefined
ORANGE                          P-P       2       Active
TEAL                            P-P       0       InActive
```

Related Commands

Command	Description
ethernet evc *evc-id*	Defines an EVC and enters EVC configuration mode.

show ethernet service instance

Use the **show ethernet service instance** privileged EXEC command to display information about Ethernet customer-service instances.

show ethernet service instance [**id** *id*] [**interface** *interface-id*] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

This command is available only if your switch is running the metro IP access or metro access image.

Syntax Description

id *id*	(Optional) Display information for the specified service-instance identifier, a per-interface service identifier that does not map to a VLAN. The range is 1 to 4294967295.
interface *interface-id*	(Optional) Display service-instance information for the specified interface.
detail	(Optional) Display detailed information about service instances or the specified service-instance ID or 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

Privileged EXEC

Command History

Release	Modification
12.2(25)SEG	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 ethernet service instance** command:

```
Switch# show ethernet service instance
Identifier Interface              CE-Vlans
222        FastEthernet0/1       untagged,1-4094
10         FastEthernet0/2
222        FastEthernet0/2       200
333        FastEthernet0/2       default
10         FastEthernet0/3       300
11         FastEthernet0/3
10         FastEthernet0/4       300
10         FastEthernet0/6       untagged,1-4094
10         FastEthernet0/7       untagged,1-4094
10         FastEthernet0/8       untagged,1-4094
10         FastEthernet0/9       untagged
20         FastEthernet0/9
222        FastEthernet0/11      300-350,900-999
```

```
333         FastEthernet0/11      100-200,1000,1999-4094
222         FastEthernet0/12      20
333         FastEthernet0/12      10
10          FastEthernet0/13      10
20          FastEthernet0/13      20
30          FastEthernet0/13      30
200         FastEthernet0/13      222
200         FastEthernet0/14      200,222
300         FastEthernet0/14      333
555         FastEthernet0/14      555
```

Related Commands

Command	Description
service instance *id* **ethernet**	Defines an Ethernet service instance and enters Ethernet service configuration mode.

show ethernet service interface

Use the **show ethernet service interface** privileged EXEC command to display interface-based information about Ethernet customer-service instances for all interfaces or a specified interface.

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

This command is available only if your switch is running the metro IP access or metro access image.

Syntax Description

interface-id	(Optional) Display service-instance information for the specified interface.
detail	(Optional) Display detailed information about service instances on all interfaces or the specified 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

Privileged EXEC

Command History

Release	Modification
12.2(25)SEG	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 outputs from the **show ethernet service interface** commands:

```
Switch# show ethernet service interface gigabitethernet0/1
Interface          Identifier
GigabitEthernet0/1 PE2-G101

Switch# show ethernet service interface detail
Interface: FastEthernet0/1
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/2
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/3
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing

<output truncated>
```

```
Interface: GigabitEthernet0/1
ID: PE2-G101
CE-VLANS: 10,20,30
EVC Map Type: Bundling-Multiplexing
Associated EVCs:
EVC-ID CE-VLAN
WHITE 30
RED 20
BLUE 10
Associated Service Instances:
Service-Instance-ID CE-VLAN
10 10
20 20
30 30
```

Related Commands

Command	Description
service instance *id* **ethernet**	Defines an Ethernet service instance and enters Ethernet service configuration mode from interface configuration mode.

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. 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(25)EX	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. 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
---------  -------- -------- -------- --------    ------- -------
Gi0/1      Unsupp.  Unsupp.  off      off         0       0
Gi0/2      desired  off      off      off         0       0
Gi0/3      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 interface gigabitethernet0/2
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/2      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 a Gigabit Ethernet interface.

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

Syntax Description

interface *interface-id*	Display the IDPROM information for the specified Gigabit Ethernet interface.
detail	(Optional) Display detailed 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(25)EX	This command was introduced.

Usage Guidelines

This command applies only to Gigabit Ethernet interfaces and displays information about SFPs inserted in the SFP module slot.

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** command for a Gigabit Ethernet interface:

Switch# **show idprom interface gigabitethernet0/1**

```
General SFP Information
---------------------------------------------
Identifier            :   0x03
Connector             :   0x07
Transceiver           :   0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Encoding              :   0x02
BR_Nominal            :   0x01
Vendor Name           :   CISCO-NEC
Vendor Part Number    :   OD-BP1511-23SL2
Vendor Revision       :   0x30 0x30 0x30 0x31
Vendor Serial Number  :   NEC08440067
---------------------------------------------
```

```
Other Information
----------------------------------------------------------
Port asic num          : 0
Port asic port num     : 0
XCVR init completed    : 1
Embedded PHY           : not present
SFP presence index     : 0
SFP iter cnt           : 697918

SFP failed oper flag   : 0x0
IIC error cnt          : 0
IIC error dsb cnt      : 0
IIC max sts cnt        : 4
Chk for link status    : 1
Link Status            : 1
Link Status Media      : 1
Preferred media        : 0
Resolved Media         : 1
Config Media           : 1
Access Count           : 0
Access Count Max       : 2
Port Rx Loss           : no
Port Tx Fault          : no
Port Tx Disable        : no

Sfp selection asic reg map
--------------------------------
stbi                  : 0x00
sfpControl            : 0x4C
Regs Loc              : 0xF0000000

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

 Page 0 Registers
------------------------------------------------------------------------------
 0000: 1140 Control Register                      :  0001 0001 0100 0000
 0001: 6149 Control STATUS                        :  0110 0001 0100 1001
 0002: 0141 Phy ID 1                              :  0000 0001 0100 0001
 0003: 0C92 Phy ID 2                              :  0000 1100 1001 0010
 0004: 01E1 Auto-Negotiation Advertisement        :  0000 0001 1110 0001
 0005: 0000 Auto-Negotiation Link Partner         :  0000 0000 0000 0000
 0006: 0004 Auto-Negotiation Expansion Reg        :  0000 0000 0000 0100
 0007: 2001 Next Page Transmit Register           :  0010 0000 0000 0001
 0008: 0000 Link Partner Next page Registe        :  0000 0000 0000 0000
 0009: 0F00 1000BASE-T Control Register           :  0000 1111 0000 0000
 000A: 0000 1000BASE-T Status Register            :  0000 0000 0000 0000
 000F: 0000 Extended Status Register              :  0000 0000 0000 0000
 0010: 6028 PHY Specific Control Register         :  0110 0000 0010 1000
 0011: 6CC8 PHY Specific Status Register          :  0110 1100 1100 1000
 0012: 0000 Interrupt Enable Register             :  0000 0000 0000 0000
 0013: 0700 PHY Specific Status Register2         :  0000 0111 0000 0000
 0015: 01C0 Receive Error Counter                 :  0000 0001 1100 0000

 0016: 0000 Page Address Register                 :  0000 0000 0000 0000
 001A: 8040 PHY Specific Control Register2        :  1000 0000 0100 0000

<output truncated>
```

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

Syntax Description

interface-id	(Optional) Valid interfaces include physical ports (including type, 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.
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. The only valid module number is 1. This option is not available if you have 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) and private VLAN promiscuous ports. A promiscuous port must be a network node interface (NNI). This keyword is visible only when the switch is running the metro access or metro IP access image.
stats	(Optional) Display the input and output packets by switching path for the interface.
status	(Optional) Display the status of the interface. A status of *unsupported* in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
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. This keyword is visible only when the switch is running the metro access or metro IP access image.
transceiver [**detail** | **properties**]	(Optional) Display the physical properties of a CWDM[1] or DWDM[2] small form-factor (SFP) module interface. The keywords have these meanings: • **detail—**(Optional) Display calibration properties, including high and low numbers and any alarm information. • **properties—**(Optional) Display speed and duplex settings on an interface.

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.

1. coarse wavelength-division multiplexer
2. dense wavelength-division multiplexer

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)EX	This command was introduced.

Usage Guidelines

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

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

```
Switch# show interfaces gigabitethernet0/2
GigabitEthernet0/2 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.

GigabitEthernet0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/2
                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 gigabitethernet0/2 capabilities
GigabitEthernet0/2
  Model:                 ME-3400-24T-FA
  Type:                  10/100/1000BaseTX SFP
  Speed:                 10,100,1000,auto
  Duplex:                half,full,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on,desired),tx-(none)
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),tx-(4q2t)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
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 gigabitethernet0/2 description
Interface Status         Protocol Description
Gi0/2       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 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
Fa0/1                        connected    1          a-full  a-100 10/100BaseTX
Fa0/2                        connected    1          a-full  a-100 10/100BaseTX
Fa0/3                        notconnect   1            auto   auto 10/100BaseTX
Fa0/4                        disabled     1            auto   auto 10/100BaseTX
Fa0/5                        disabled     1            auto   auto 10/100BaseTX
Fa0/6                        disabled     1            auto   auto 10/100BaseTX
Fa0/7                        disabled     1            auto   auto 10/100BaseTX
Fa0/8                        disabled     1            auto   auto 10/100BaseTX
Fa0/9                        disabled     1            auto   auto 10/100BaseTX
Fa0/10                       disabled     1            auto   auto 10/100BaseTX
Fa0/11                       disabled     1            auto   auto 10/100BaseTX
```

```
Fa0/12                      disabled     1            auto   auto 10/100BaseTX
Fa0/13                      disabled     1            auto   auto 10/100BaseTX
Fa0/14                      disabled     1            auto   auto 10/100BaseTX
Fa0/15                      disabled     1            auto   auto 10/100BaseTX
Fa0/16                      disabled     1            auto   auto 10/100BaseTX
Fa0/17                      disabled     1            auto   auto 10/100BaseTX
Fa0/18                      disabled     1            auto   auto 10/100BaseTX
Fa0/19                      disabled     1            auto   auto 10/100BaseTX
Fa0/20                      disabled     1            auto   auto 10/100BaseTX
Fa0/21                      disabled     1            auto   auto 10/100BaseTX
Fa0/22                      disabled     1            auto   auto 10/100BaseTX
Fa0/23                      disabled     1            auto   auto 10/100BaseTX
Fa0/24                      disabled     1            auto   auto 10/100BaseTX
Gi0/1                       notconnect   1            auto   auto 10/100/1000Ba
seTX SFP
Gi0/2                       connected    vl-err-dis a-full a-1000 10/100/1000BaseTX
```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25.

```
Switch# show interfaces fastethernet0/22 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/22                       connected    20,25      a-full  a-100 10/100BaseTX
```

In this example, port 2 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20.

```
Switch# show interfaces gigabitethernet0/2 status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/2                        connected    20         a-full  a-100 10/100/1000BaseTX
```

This is an example of output from the **show interfaces status err-disabled** command for an interface:

```
Switch# show interfaces gigabitethernet0/2 status err-disabled

Port      Name               Status       Reason               Err-disabled Vlans
Gi0/2                        connected    elmi evc down        1,200
```

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

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

```
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
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: none
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
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: none
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Table 2-11 show interfaces switchport Field Descriptions

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational modes.
Administrative Trunking Encapsulation 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	Lists the VLAN ID of the trunk that is in native mode.
Administrative Native VLAN tagging	Displays whether or not VLAN tagging 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.
Trunking VLANs enabled	Lists the active VLANs on the trunk.
Capture VLANs allowed	Lists the allowed VLANs on the trunk.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.

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 gigabitethernet0/2 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
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 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 switchport 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 output from the **show interfaces** *interface-id* **trunk** command. It displays trunking information for the port.

```
Switch# show interfaces gigabitethernet0/1 trunk
Port          Mode         Encapsulation  Status        Native vlan
Gi0/1         auto         negotiate      trunking      1

Port          Vlans allowed on trunk
Gi0/1         1-4094

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

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

This is an example of output from the **show interfaces transceiver properties** command. If you do not specify an interface, the output of the command shows the status on all switch ports:

```
Switch# show interfaces transceiver properties
Name : Fa0/1
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 100
Operational Duplex: full
Operational Auto-MDIX: on

Name : Fa0/2
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 100
Operational Duplex: full
Operational Auto-MDIX: on

<output truncated>
```

Related Commands

Command	Description
switchport access vlan	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 mode private-vlan	Defines private-VLAN association for a host port or private-VLAN mapping for a promiscuous port.

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** | **trunk**] [**module** *switch- number*] | **etherchannel** | **protocol status**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the physical interface, including type, module, and port number.
errors	(Optional) Display error counters.
trunk	(Optional) Display trunk counters.
module *switch- number*	**Note** (Optional) Display counters for the specified switch number. The only available value is 1.
etherchannel	(Optional) Display EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
protocol status	(Optional) Display status of protocols enabled on interfaces.
| 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(25)EX	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
Fa0/1                  0              0              0              0
Fa0/2                  0              0              0              0

<output truncated>
```

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

```
Switch# show interfaces counters protocol status
Protocols allocated:
 Vlan1: Other, IP
 Vlan20: Other, IP, ARP
 Vlan30: Other, IP, ARP
 Vlan40: Other, IP, ARP
 Vlan50: Other, IP, ARP
 Vlan60: Other, IP, ARP
 Vlan70: Other, IP, ARP
 Vlan80: Other, IP, ARP
 Vlan90: Other, IP, ARP
 Vlan900: Other, IP, ARP
 Vlan3000: Other, IP
 Vlan3500: Other, IP
 FastEthernet0/1: Other, IP, ARP, CDP
 FastEthernet0/2: Other, IP
 FastEthernet0/3: Other, IP
 FastEthernet0/4: Other, IP
 FastEthernet0/5: Other, IP
 FastEthernet0/6: Other, IP
 FastEthernet0/7: Other, IP
 FastEthernet0/8: Other, IP
 FastEthernet0/9: Other, IP
 FastEthernet0/10: 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
Gi0/1               0              0           0
Gi0/2               0              0           0
Gi0/3           80678           4155           0
Gi0/4           82320            126           0
Gi0/5               0              0           0

<output truncated>
```

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.

show 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. For example, enter the interface (such as gigabitethernet 0/x) into which a small form-factor pluggable (SFP) module is installed to display its identity.
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(25)EX	This command was introduced.
12.2(25)SEG1	Support for the *entity-name* keyword was added.

Usage Guidelines

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

Many legacy SFPs are not programmed with PIDs and VID.s

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: "ME-3400-24TS-A"
PID: ME-3400-24TS-A , VID:Vo1 , SN: FSJC0407839

NAME: "GigabitEthernet0/1", DESCR: "100BaseBX-10U SFP"
PID:                      , VID:    , SN: NEC08440067

NAME: "GigabitEthernet0/2", DESCR: "10/100/1000BaseTX SFP"
PID:                      , VID:    , SN: 00000MTC0839048G
```

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*]

Note This command is available only if your switch is running the metro IP access or metro access image.

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(25)EX	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 interfaces** command:

```
Switch# show ip arp inspection interfaces
 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi0/1            Untrusted              15                 1
 Gi0/2            Untrusted              15                 1
 Gi0/3            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 gigabitethernet0/1
 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Gi0/1            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
----------  ----  --------------  ---------------  ---------  -----------  ----
Gi0/1       5     0003.0000.d673  192.2.10.4               5  DHCP Deny    19:39:01 UTC
Mon Mar 1 1993
Gi0/1       5     0001.0000.d774  128.1.9.25               6  DHCP Deny    19:39:02 UTC
Mon Mar 1 1993
Gi0/1       5     0001.c940.1111  10.10.10.1               7  DHCP Deny    19:39:03 UTC
Mon Mar 1 1993
Gi0/1       5     0001.c940.1112  10.10.10.2               8  DHCP Deny    19:39:04 UTC
Mon Mar 1 1993
Gi0/1       5     0001.c940.1114  173.1.1.1               10  DHCP Deny    19:39:06 UTC
Mon Mar 1 1993
Gi0/1       5     0001.c940.1115  173.1.1.2               11  DHCP Deny    19:39:07 UTC
Mon Mar 1 1993
Gi0/1       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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
GigabitEthernet0/1               yes         unlimited
GigabitEthernet0/2               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(25)EX	This command was introduced.

Usage Guidelines

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

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

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    GigabitEthernet0/1
00:D0:B7:1B:35:DE   10.1.2.151       237         dhcp-snooping  20    GigabitEthernet0/2
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    GigabitEthernet0/1
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    GigabitEthernet0/2
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 gigabitethernet0/2
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:30:94:C2:EF:35   10.1.2.151       290         dhcp-snooping  20    GigabitEthernet0/2
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    GigabitEthernet0/1
00:00:00:00:00:02   10.1.2.151       65          dhcp-snooping  20    GigabitEthernet0/2
Total number of bindings: 2
```

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

Table 2-12 show ip dhcp snooping binding Command Output

Field	Description
MacAddress	Client hardware MAC address
IpAddress	Client IP address assigned from the DHCP server
Lease(sec)	Remaining lease time for the IP address
Type	Binding type
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host
Total number of bindings	Total number of bindings configured on the switch **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(25)EX	This command was introduced.

Examples

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

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

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

Last 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(37)SE	This command was introduced.

Usage Guidelines

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

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

Table 2-13 DHCP Snooping Statistics

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the **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 2-13 DHCP Snooping Statistics

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(25)EX	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*] **[detail]**] [**vlan** *vlan-id*] **[detail]** [| {**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(25)EX	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.

Although visible in the output display, output lines for source-only learning are not valid.

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
```

Note Source-only learning are not supported, and information appearing for this feature is not valid.

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

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping (minimal)  : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
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 and configures IGMP snooping on the switch or on a VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
show ip igmp snooping 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-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(25)EX	This command was introduced.

Usage Guidelines

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

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

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
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/2
104       224.1.4.3       igmp        v2          Gi0/1, Gi0/2
```

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          Gi0/1, Fa0/15
104       224.1.4.3       igmp        v2          Gi0/1, Fa0/15
```

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          Gi0/1, Fa0/15
```

Related Commands

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

show 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(25)EX	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    Gi0/1(dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan mrouter	Adds a multicast router port to a multicast VLAN.
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** user EXEC command to display the IP address and incoming port for the Internet Group Management Protocol (IGMP) query most recently received by the switch.

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

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Display querier information as well as configuration and operational information pertaining to the querier.
| 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(25)EX	This command was introduced.

Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and IP address of a detected device (also called a *querier*) that sends IGMP query message. 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 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 detail** command displays the IP address of the most recent device detected by the switch querier along with 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                  Gi0/1
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              Fa0/1

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 Fa0/1
---------------------------------------------------------
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 querier	Enables and configures the IGMP snooping querier on the switch or on a VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

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

Note This command is available only if your switch is running the metro IP access or metro access image.

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.
vlan *vlan-id*	(Optional) Display IP source bindings on a specific VLAN.
interface *interface-id*	(Optional) Display IP source bindings 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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch> show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
--------------      ---------------  ----------  -------------  ----  --------------------
00:00:00:0A:00:0B   11.0.0.1         infinite    static         10    GigabitEthernet0/1
00:00:00:0A:00:0A   11.0.0.2         10000       dhcp-snooping  10    GigabitEthernet0/1
```

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*]

Note This command is available only if your switch is running the metro IP access or metro access image.

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(25)EX	This command was introduced.

Examples

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

```
Switch> show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa0/1      ip           active       10.0.0.1                         10
fa0/1      ip           active       deny-all                         11-20
fa0/2      ip           inactive-trust-port
fa0/3      ip           inactive-no-snooping-vlan
fa0/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
fa0/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
fa0/4      ip-mac       active       deny-all         deny-all        12-20
fa0/5      ip-mac       active       10.0.0.3         permit-all      10
fa0/5      ip-mac       active       deny-all         permit-all      11-20
```

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

- On the Fast Ethernet 0/1 interface, dynamic host control protocol (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 is on the interface. For VLANs 11 to 20, the second entry shows that a default port access control list (ACL) is applied on the interface for the VLANs on which IP source guard is not configured.
- The Fast Ethernet 0/2 interface is configured as trusted for DHCP snooping.
- On the Fast Ethernet 0/3 interface, DHCP snooping is not enabled on the VLANs to which the interface belongs.

- On the Fast Ethernet 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 Fast Ethernet 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 gigabitethernet0/6
IP source guard is not configured on the interface gi0/6.
```

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.

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

Note This command is available only if your switch is running the metro IP access image.

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 participating IPC zones. The switch supports one 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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

This 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 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*]

Note This command is available only if your switch is running the metro IP access or metro access image.

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 64.
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(25)EX	This command was introduced.

Usage Guidelines

After enabling Layer 2 protocol tunneling on an access port, a trunk port, or an 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
---------- -------- --------- --------- ------------- ------------- -------------
  Fa0/3     ---           ----      ----          ----          ----          ----
            ---           ----      ----          ----          ----          ----
            ---           ----      ----          ----          ----          ----
            pagp          ----      ----             0        242500
            lacp          ----      ----         24268        242640
            udld          ----      ----             0        897960
  Fa0/4     ---           ----      ----          ----          ----          ----
            ---           ----      ----          ----          ----          ----
            ---           ----      ----          ----          ----          ----
            pagp          1000      ----         24249        242700
            lacp          ----      ----         24256        242660
            udld          ----      ----             0        897960
  Gi0/1     cdp           ----      ----        134482       1344820
            ---           ----      ----          ----          ----          ----
            ---           ----      ----          ----          ----          ----
            pagp          1000      ----             0        242500
            lacp           500      ----             0        485320
            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)
------- ----------- ---------------- ---------------- ----------
  Fa0/2  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld ----/----/----   ----/----/----
  Fa0/3  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld 1000/----/----   ----/----/----
  Fa0/4  --- --- --- ----/----/----   ----/----/----   up
     pagp lacp udld 1000/ 500/----   ----/----/----
  Fa0/5  cdp stp vtp ----/----/----   ----/----/----   down
     ---- ---- ---- ----/----/----   ----/----/----
  Gi0/1  --- --- --- ----/----/----   ----/----/----   down
     pagp ---- ---- ----/----/----   1000/----/----
  Gi0/2  --- --- --- ----/----/----   ----/----/----   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*]

Note LACP is available only on network node interfaces (NNIs).

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(25)EX	This command was introduced.

Usage Guidelines

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

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

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

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. Table 2-14 describes the fields in the display.

```
Switch> show lacp counters
               LACPDUs          Marker       Marker Response    LACPDUs
Port          Sent    Recv     Sent    Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------------
Channel group:1
Gi0/1         19      10       0       0        0       0         0
Gi0/2         14      6        0       0        0       0         0
```

Table 2-14 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
Gi0/1       SA      bndl    32768         0x3       0x3     0x4      0x3D
Gi0/2       SA      bndl    32768         0x3       0x3     0x5      0x3D
```

Table 2-15 describes the fields in the display.

Table 2-15 show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: • – —Port is in an unknown state. • **bndl**—Port is attached to an aggregator and bundled with other ports. • **susp**—Port is in a suspended state; it is not attached to any aggregator. • **hot-sby**—Port is in a hot-standby state. • **indiv**—Port is incapable of bundling with any other port. • **indep**—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). • **down**—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports s in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port number.
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired **Note** In the above list, 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
Gi0/1     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
Gi0/2     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** global configuration command to display the link-state group information.

show link state group [*number*] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Note This command is available only if your switch is running the metro IP access or metro access image.

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(25)SEG	This command was introduced.

Usage Guidelines

Use the **show link state group** command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group.

Enter the **detail** keyword to display detailed information about the group. The output for the **show link state group detail** command displays only those link-state groups that have link-state tracking enabled or that have upstream or downstream interfaces (or both) configured. If there is no link-state group configuration for a group, it is not shown as enabled or disabled.

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 : Gi0/15(Dwn) Gi0/16(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn) Gi0/17(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(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 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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mac-access group** user EXEC command. In this display, Fast Ethernet interface 0/2 has the MAC access list *macl_e1* applied to inbound traffic; no MAC ACLs are applied to other interfaces.

```
Switch> show mac access-group
Interface FastEthernet0/1:
   Inbound access-list is macl_e1
   Outbound access-list is not set
Interface FastEthernet0/2:
   Inbound access-list is not set
   Outbound access-list is not set
Interface FastEthernet0/3:
   Inbound access-list is not set
   Outbound access-list is not set
Interface FastEthernet0/4:
   Inbound access-list is not set
   Outbound access-list is not set
Interface FastEthernetv0/5:
   Inbound access-list is not set
   Outbound access-list is not set
<output truncated>
```

This is an example of output from the **show mac access-group interface fastethernet0/1** command:

```
Switch# show mac access-group interface fastethernet0/1
Interface FastEthernet0/1:
   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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch> show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
 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    Gi0/4
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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

Related Commands

Command	Description
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(25)EX	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(25)EX	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
Switch# show mac address-table count
Mac Entries for Vlan   : 1
---------------------------
Dynamic Address Count  : 2
Static  Address Count  : 0
Total Mac Addresses    : 2
```

Related Commands

Command	Description
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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

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

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch> show mac address-table interface gigabitethernet0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
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*]

Note This command is supported only when the switch is running the metro IP access or metro access image.

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(25)EX	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 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**]

Note This command is supported only when the switch is running the metro IP access or metro access image.

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(25)SEG	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(25)EX	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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

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

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0100.0ccc.cccc  STATIC  CPU
 All    0180.c200.0000  STATIC  CPU
 All    0100.0ccc.cccd  STATIC  CPU
 All    0180.c200.0001  STATIC  CPU
 All    0180.c200.0004  STATIC  CPU
 All    0180.c200.0005  STATIC  CPU
   4    0001.0002.0004  STATIC  Drop
   6    0001.0002.0007  STATIC  Drop
Total Mac Addresses for this criterion: 8
```

Related Commands

Command	Description
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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

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

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.0ccc.cccc  STATIC  CPU
   1    0180.c200.0000  STATIC  CPU
   1    0100.0ccc.cccd  STATIC  CPU
   1    0180.c200.0001  STATIC  CPU
   1    0180.c200.0002  STATIC  CPU
   1    0180.c200.0003  STATIC  CPU
   1    0180.c200.0005  STATIC  CPU
   1    0180.c200.0006  STATIC  CPU
   1    0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 9
```

Related Commands

Command	Description
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 monitor

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)EX	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
Switch# show monitor
Session 1
---------
 Type       :Local Session
Source Ports:
    RX Only:      Fa0/24
    TX Only:      None
    Both:         Fa0/1-2,Fa0/1-5
Destination Ports:Fa0/18
    Encapsulation:Replicate

Session 2
---------
 Type       :Remote Source Session
Source Ports:
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 RSPAN source session 1:

```
Switch# show monitor session 1
Session 1
---------
 Type       :Local Session
Source Ports:
    RX Only:      Fa0/24
    TX Only:      None
    Both:         Fa0/1-2,Fa0/1-5
Destination Ports:Fa0/18
    Encapsulation:Replicate
```

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           :Fa0/2
Destination Ports :Fa0/3
    Encapsulation :Replicate
          Ingress:Enabled, default VLAN = 5
    Ingress encapsulation:DOT1Q

Session 2
---------
Type               :Local Session
Source Ports       :
    Both           :Fa0/1
Destination Ports :Fa0/4
    Encapsulation :Replicate
          Ingress:Enabled
    Ingress encapsulation:DOT1Q
```

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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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, 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(25)EX	This command was introduced.
12.2(35)SE	The Mode and VLAN fields were added to the output display.

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 **show mvr interface** *interface-id* command and the specified port is a non-MVR port, the output displays NON MVR in the Type field. For active MVR ports, it displays the port type (RECEIVER or SOURCE), mode (access or trunk), VLAN, status, and Immediate-Leave setting.

If you enter the **members** keyword, all MVR group members on the 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 mvr interface** command:

```
Switch# show mvr interface
Port    Type            Mode            VLAN    Status          Immediate Leave
----    ----            ----            ----    -------         ---------------
Fa0/1   Receiver        Trunk           1       ACTIVE/UP       DISABLED
Fa0/1   Receiver        Trunk           2000    ACTIVE/DOWN     DISABLED
Fa0/2   Receiver        Trunk           2       ACTIVE/UP       DISABLED
Fa0/2   Receiver        Trunk           3000    ACTIVE/UP       DISABLED
Fa0/3   Receiver        Trunk           2       ACTIVE/UP       DISABLED
Fa0/3   Receiver        Trunk           3000    ACTIVE/UP       DISABLED
Fa0/10  Source          Access          10      ACTIVE/UP       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 fastethernet0/10** command:

```
switch# show mvr interface fa0/10
Port    Type            Mode            VLAN    Status          Immediate Leave
----    ----            ----            ----    -------         ---------------
Fa0/10  RECEIVER        Trunk           201     ACTIVE/DOWN     DISABLED
```

This is an example of output from the **show mvr interface fastethernet0/1** command. In this example, the port is not an MVR member:

```
switch# show mvr interface fa0/1
Port    Type            Mode            VLAN    Status          Immediate Leave
----    ----            ----            ----    -------         ---------------
Fa0/1   NON MVR         Access          0       INACTIVE        DISABLED
```

This is an example of output from the **show mvr interface gigabitethernet0/1 members** command:

```
Switch# show mvr interface gigabitethernet0/1 members
239.255.0.0     vlan 202     DYNAMIC ACTIVE
239.255.0.1     vlan 202     DYNAMIC ACTIVE
239.255.0.2     vlan 202     DYNAMIC ACTIVE
239.255.0.3     vlan 203     DYNAMIC ACTIVE
239.255.0.4     vlan 203     DYNAMIC ACTIVE
239.255.0.5     vlan 203     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(25)EX	This command was introduced.
12.2(35)SE	The VLAN and Membership fields were added to the output display.

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     Status   Members  VLAN   Membership
------------  ------   -------  ----   ----------
239.1.1.1     ACTIVE   Fa0/1    1      Static
239.1.1.1     ACTIVE   Fa0/1    2000   Static
239.1.1.1     ACTIVE   Fa0/2    2      Static
239.1.1.1     ACTIVE   Fa0/2    3000   Static
239.1.1.2     ACTIVE   Fa0/1    1      Static
239.1.1.2     ACTIVE   Fa0/2    2      Static

<output truncated>
```

This is an example of output from the **show mvr members 239.255.0.2** command. It shows how to view the members of the IP multicast group 239.255.0.2:

```
Switch# show mvr members 239.255.0.2
239.255.0.2     ACTIVE          Gi0/1(d), Gi0/2(d), Gi0/3(d),
                                Gi0/4(d), Gi0/5(s)
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **members** keyword is appended to the command.

show pagp

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

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

Note PAgP is available only on network node interfaces (NNIs).

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.
| 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(25)EX	This command was introduced.

Usage Guidelines

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

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* 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
  Gi0/1       45     42       0      0
  Gi0/2       45     41       0      0
```

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

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

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/1       SC    U6/S7   H       30s      1        128        Any      16
Gi0/2       SC    U6/S7   H       30s      1        128        Any      16
```

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

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

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

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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

This is a partial output example from the **show parser macro** command:

```
Switch# show parser macro
Total number of macros = 2
------------------------------------------------------------------
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
------------------------------------------------------------------
Macro name : test1
Macro type : customizable
no shutdown
flowcontrol receive on
speed 100
------------------------------------------------------------------
```

This is an example of output from the **show parser macro name** command:

```
Switch# show parser macro name sample-macro1
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
```

This is an example of output from the **show parser macro brief** command:

```
Switch# show parser macro brief
    customizable     : sample-macro1
    customizable     : test1
```

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 policer aggregate

Use the **show policer aggregate** user EXEC command to display quality of service (QoS) aggregate policer information for all aggregate policers or a specific policer.

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

Syntax Description

aggregate-policer-name	(Optional) The name of the aggregate 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.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)EX	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 policer aggregate** command:

```
Switch> show policer aggregate my-policer
aggregate-policer: my-policer

     police cir 12000000 bc 5000
       conform-action transmit
       exceed-action set-cos-transmit cos table 67577

In use by policymap: pin
```

Related Commands

Command	Description
police aggregate (policy-map class configuration)	Applies an aggregate policer to multiple classes in the same policy map.
policer aggregate (global configuration)	Creates an aggregate policer to police all traffic received on an interface.

show policer cpu uni

Use the **show policer cpu uni** user EXEC command to display control-plane policer information for the switch, including frames dropped or the configured threshold rate for the control-plane security feature on the switch.

show policer cpu uni [**drop** [*policer-number*] | **rate**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

drop	(Optional) Display control-plane frame-drop count for the specified policer number or for all control-plane policers (0 to 26).
policer *number*	(Optional) Display drop statistics for a specific user network interface (UNI) policer number. The range is from 0 to 26.
rate	(Optional) Display the configured threshold rate for CPU policers.
| 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(25)EX	This command was introduced.
12.2(25)SEG1	Outputs for the **show policer cup uni drop** changed.

Usage Guidelines

The **show policer cpu uni drop** privileged EXEC command displays the number of accepted and dropped frames for all policers on the switch or for the specified policer number.

The **show policer cpu uni rate** command displays the CPU protection rate-limit threshold on the switch that was configured by entering the **policer cpu uni** *rate* global configuration command or the default rate of 16000 bits per second (bps).

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 policer cpu uni drop** command. Note that CPU protection only uses policers 0 to 26.

```
Switch# show policer cpu uni drop
================================
Port                    In           Dropped
Name                  Frames          Frames
========================================
Port                    In           Dropped
Name                  Frames          Frames
Fa0/1                  300              0
Fa0/2                    0              0
Fa0/3                    0              0
Fa0/4                    0              0
Fa0/5                  200              0
Fa0/6                    0              0
Fa0/7                    0              0
Fa0/8                    0              0
Fa0/9               508055         325086
Fa0/10                   0              0
Fa0/11                   0              0
Fa0/12                   0              0
Fa0/13                   0              0
Fa0/14                   0              0
Fa0/15                   0              0
Fa0/16                   0              0
Fa0/17                   0              0
Fa0/18                   0              0
Fa0/19                   0              0
Fa0/20                   0              0
Fa0/21                   0              0
Fa0/22                   0              0
Fa0/23                   0              0
Fa0/24                   0              0
Gi0/1                    0              0
Gi0/2                    0              0
drop-all                 0        1849645
```

This is an example of the new output format for the **show policer cpu uni drop interface** command:

```
Switch# show policer cpu uni drop interface gigabitethernet 0/1
============================
Policer assigned for Gi0/2
============================
Protocols using this policer:
"VTP" "CISCO_L2" "KEEPALIVE" "SWITCH_IGMP" "SWITCH_L2PT"
Policer rate: 160000 bps
In frames: 48014
Drop frames: 28630
```

This is an example of output from the **show policer cpu uni rate** command when the default rate is used.

```
Switch> show policer cpu uni rate
CPU UNI port police rate = 160000 bps
```

Related Commands

Command	Description
policer cpu uni	Configures a CPU policer threshold rate for the switch.
show platform policer cpu	Displays allocated policer indexes and the corresponding features for all ports or the specified port.

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 and outgoing traffic and the actions to be performed on the classified traffic.

show policy-map [*policy-map-name* | **interface** [*interface-id*] [**input** | **output**] [**class** *class-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 an individual class.
interface [*interface-id*] [**input** | **output**]	(Optional) Display information and statistics about policy maps applied to all ports or the specified port. If you specify a port, you can specify additional keywords.The keywords have these meanings: • *interface-id*—Display information about policy maps on the specified physical interface. • **input**—Display information about input policy maps on the switch or applied to the specified port. • **output**—Display the information about output policy-maps on the switch or applied to the specified port.
class *class-name*	(Optional) Display policy-map statistics for an 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.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

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

 Policy Map mypolicy
  class  dscp5
```

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

```
Switch> show policy-map top2
  Policy Map top2
    Class class-default
      shape average 11111124
      service-policy pout
```

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

```
Switch> show policy-map pout
  Policy Map pout
    Class ip1
      priority
     police cir percent 10
       conform-action transmit
       exceed-action drop
      queue-limit 250
      queue-limit precedence  1 100
    Class ip2
      Average Rate Traffic Shaping
      cir 5%
    Class ip3
      bandwidth percent 10
      queue-limit 200
      queue-limit precedence  3 100
```

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

```
Switch> show policy-map pin-police
Policy Map pin-police
    Class ip1
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
```

This is an example of output from the **show policy-map interface** command for an interface with a two-level output policy map applied:

```
Switch> show policy-map interface fastethernet0/3
 FastEthernet0/3

  Service-policy output: top2

    Class-map: class-default (match-any)
      209871 packets
      Match: any
        56 packets
      Traffic Shaping
        Average Rate Traffic Shaping
        CIR 11111124 (bps)
      Output Queue:
        Tail Packets Drop: 195421

      Service-policy : pout

        Class-map: ip1 (match-all)
          9309 packets
          Match: ip precedence 1
          Priority
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
      conform: 4916 (packets) exceed: 4393 (packets)
```

```
      Queue Limit
        queue-limit 250 (packets)
        queue-limit precedence  1 100 (packets)
      Output Queue:
        Max Tail Drop Threshold: 250
        Tail Packets Drop: 4393

    Class-map: ip2 (match-all)
      0 packets
      Match: ip precedence 2
      Traffic Shaping
        Average Rate Traffic Shaping
        CIR 5%       555555 (bps)
      Output Queue:
        Max Tail Drop Threshold: 48
        Tail Packets Drop: 0

    Class-map: ip3 (match-all)
      0 packets
      Match: ip precedence 3
      Bandwidth percent 10         1111110 (bps)
      Queue Limit
        queue-limit 200 (packets)
        queue-limit precedence  3 100 (packets)
      Output Queue:
        Max Tail Drop Threshold: 200
        Tail Packets Drop: 0

    Class-map: class-default (match-any)
      200562 packets
      Match: any
        56 packets
      Output Queue:
        Tail Packets Drop: 191028
```

This is an example of output from the **show policy-map interface** command for an interface with an input policy applied:

```
Switch> show policy-map interface gigabitethernet0/1
 GigabitEthernet0/1

  Service-policy input: pin-police

    Class-map: ip1 (match-all)
      0 packets
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
      conform: 27927 (packets) exceed: 272073 (packets)

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets
        5 minute rate 0 bps
```

Table 2-16 describes the fields in the **show policy-map interface** display. The fields in the table are grouped according to the relevant QoS feature.

Table 2-16 show policy-map interface Field Descriptions

Field	Description
Fields associated with classes or service policies	
Service-policy input/output	Name of the input or output service policy applied to the specified interface.
Class-map	Class of traffic shown. Output appears for each configured class in the policy. The choice for implementing class matches (match-all or match-any) might also appear next to the traffic class.
packets	Number of packets identified as belonging to the traffic class.
Match	Match criteria specified for the class of traffic. This includes criteria such as class of service (CoS) value, IP precedence value, Differentiated Services Code Point (DSCP) value, access groups, and QoS groups.
Fields associated with policing	
police	Shown when the **police** command has been configured to enable traffic policing. Displays the specified committed information rate (CIR) and conform burst size (BC) used for policing packets.
conform-action	Displays the action to be taken on packets marked as conforming to a specified rate.
conform	Displays the number of packets marked as conforming to the specified rate.
exceed-action	Displays the actions to be taken on packets marked as exceeding a specified rate.
exceed	Displays the number of packets marked as exceeding the specified rate.
Fields associated with queuing	
Queue Limit	Queue size configured for the class in number of packets.
Output Queue	The queue created for this class of traffic.
Tail packets dropped	The number of packets dropped when the mean queue depth is greater than the maximum threshold value.
Fields associated with traffic scheduling	
Traffic shaping	The rate used for shaping traffic.
Bandwidth	Bandwidth configured for this class in kbps or a percentage.
Priority	Indicates that this class is configured for priority queuing.

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, 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(25)EX	This command was introduced.

Usage Guidelines

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

If you enter an *interface-id*, the command displays port security settings for the interface.

If you enter the **address** keyword, the command displays the secure MAC addresses for all interfaces and the aging information for each secure address.

If you enter an *interface-id* and the **address** keyword, the command displays all the MAC addresses for the interface with aging information for each secure address. You can also use this command to display all the MAC addresses for an interface even if you have not enabled port security on it.

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

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

Examples

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

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
-------------------------------------------------------------------------------
     Gi0/1         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 gigabitethernet0/1
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    Gi0/2       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 gigabitethernet0/2 address** command:

```
Switch# show port-security interface gigabitethernet0/2 address
          Secure Mac Address Table
-----------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi0/2       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 gigabitethernet0/2 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 port-type

Use the **show port-type** privileged EXEC command to display interface type information for the Cisco ME switch.

show port-type [**uni** | **nni**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

uni	User network interface.
| nni	Network node 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

Privileged EXEC

Command History

Release	Modification
12.2(25)EX	This command was introduced.

Usage Guidelines

If you enter the command without keywords, the output includes the interface type information for all ports on the switch. If you use the **uni** keyword, the output includes only the UNIs. If you use the **nni** keyword, the output includes only the NNIs.

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

Examples

This is an example of output from the **show port-type** command with no keywords:

```
Switch# show port-type
Port      Name               Vlan       Port Type
--------- ------------------ ---------- ----------------------------
Fa0/1                        1          User Network Interface (uni)
Fa0/2                        1          User Network Interface (uni)
Fa0/3                        1          User Network Interface (uni)
Fa0/4                        1          User Network Interface (uni)
Fa0/5                        1          User Network Interface (uni)
Fa0/6                        1          User Network Interface (uni)
Fa0/7                        1          User Network Interface (uni)
Fa0/8                        1          User Network Interface (uni)
Fa0/9                        1          User Network Interface (uni)
Fa0/10                       1          User Network Interface (uni)
Fa0/11                       1          User Network Interface (uni)
Fa0/12                       1          User Network Interface (uni)
Fa0/13                       1          User Network Interface (uni)
Fa0/14                       1          User Network Interface (uni)
Fa0/15                       1          User Network Interface (uni)
Fa0/16                       1          User Network Interface (uni)
```

```
Fa0/17                       routed     User Network Interface (uni)
Fa0/18                       1          User Network Interface (uni)
Fa0/19                       1          User Network Interface (uni)
Fa0/20                       1          User Network Interface (uni)
Fa0/21                       1          User Network Interface (uni)
Fa0/22                       1          User Network Interface (uni)
Fa0/23                       10         User Network Interface (uni)
Fa0/24                       10         User Network Interface (uni)
Gi0/1                        1          Network Node Interface (nni)
Gi0/2                        1          Network Node Interface (nni)
```

This is an example of output from the **show port-type** command using keywords:

```
Switch# show port-type nni | exclude Gigabitethernet0/1
Port      Name               Vlan       Port Type
--------- ------------------ ---------- ----------------------------
Gi0/2                        1          Network Node Interface (nni)
```

Related Commands

Command	Description
port-type	Changes the interface type for a specific port.

show sdm prefer

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

show sdm prefer [**default** | **layer-2**] [| {**begin** | **exclude** | **include**} *expression*]

Note The **default** keyword is visible only when the metro IP access image is installed on the switch.

Syntax Description

default	(Optional) Display the template that balances system resources among features. This template is only available with the metro IP access image.
layer-2	(Optional) Display resource allocations for the template that supports Layer 2 features and does not support routing.
| 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(25)EX	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, displaying the template in use:

```
Switch# show sdm prefer
The current template is ''layer-2'' 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 unicast IPv4 routes:                    0
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      512
  number of IPv4/MAC security aces:                 1K
```

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

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

number of unicast mac addresses:                    5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    9K
    number of directly-connected IPv4 hosts:        5K
    number of indirect IPv4 routes:                 4K
  number of IPv4 policy based routing aces:         512
  number of IPv4/MAC qos aces:                      512
  number of IPv4/MAC security aces:                 1K
```

Related Commands

Command	Description
sdm prefer	Sets the SDM template to maximize resources for Layer 2 functionality or to the default template.

show spanning-tree

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

show spanning-tree [*bridge-group* | **active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **mst** | **pathcost method** | **root** | **summary** [**totals**] | **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).
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 network node interfaces (NNIs), VLANs, and NNI port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48. **Note** Spanning Tree Protocol (STP) is not supported on user node interfaces (UNIs). If you enter a UNI interface ID, no spanning-tree information is displayed.
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 send 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 send 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 NNIs, VLANs, and NNI port channels. STP is not supported on UNIs. 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.
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(25)EX	This command was introduced.
12.2(25)SEG	The **digest** keyword was added, and new digest and transmit hold count fields appear.

Usage Guidelines

STP is not supported on UNIs. Valid spanning-tree information is available only for NNIs.

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 (GigabitEthernet0/1)
             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
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            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 (GigabitEthernet0/1), 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 (GigabitEthernet0/1) 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 gigabitethernet0/1
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 3019      128.24   P2p
```

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

```
Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
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.
```

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 configuration digest** command:

```
Switch# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision  0     Instances configured 1
Digest          0xAC36177F50283CD4B83821D8AB26DE62
Pre-std Digest  0xBB3B6C15EF8D089BB55ED10D24DF44DE
```

Thisis an example of output from the **show spanning-tree mst interface** *interface-id* command:

```
Switch# show spanning-tree mst interface gigabitethernet0/1
GigabitEthernet0/1 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    Gi0/1           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
--------------------   ---- ----- --------- ---- --------------------------------
GigabitEthernet0/1     root FWD   200000    128  P2P bound(STP)
GigabitEthernet0/2     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 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 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, 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(25)EX	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
---------    -------------  ----------  ---------  ---------
Gi0/1        Forwarding     20 pps      10 pps     5 pps
Gi0/2        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 0/1
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi0/1        Forwarding     20 pps      10 pps     5 pps
```

Table 2-17 describes the fields in the **show storm-control** display.

Table 2-17 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 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(25)EX	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.

The system MTU refers to ports operating at 10/100 Mbps; the system jumbo MTU refers to Gigabit ports; the routing MTU is the MTU for routed packets.

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
Routing MTU size is 1500 bytes
```

Related Commands

Command	Description
system mtu	Sets the MTU size for the Fast Ethernet or Gigabit Ethernet ports.

show table-map

Use the **show table-map** user EXEC command to display quality of service (QoS) table-map information about all configured table maps or the specified table map.

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

Syntax Description

table-map-name	(Optional) The name of the table 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(25)EX	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 table-map** command:

```
Switch> show table-map
tandoori_1>show table-map
 Table Map abc
    default copy

 Table Map cos2dscp
    from 2 to 16
    default copy

 Table Map cos2cos
    from 2 to 5
    from 3 to 6
    default 7

 Table Map cos2cos10
    default copy

 Table Map cos=cos
    default copy
```

This is an example of output from the **show table-map** command for a specific table map name:

```
Switch> show table-map tm

Table Map tm
    from 1 to 62
    from 2 to 63
    default ignore
```

Related Commands

Command	Description
table-map	Creates quality of service (QoS) mapping tables, such as CoS to DSCP, and so on.

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(25)EX	This command was introduced.

Usage Guidelines

If you do not enter an *interface-id*, administrative and operational UDLD status for all interfaces appear.

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

Examples

This is an example of output from the **show udld** *interface-id* command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-18 describes the fields in this display.

```
Switch> show udld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
    Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/2
    Message interval: 5
    CDP Device name: Switch-A
```

Table 2-18 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.

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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

Note Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

```
Switch> show version
Cisco IOS Software, MEAP Software (MEAP-IPSERVICES-M), Experimental Version 12.2
(20050712:084347) [teresang-meap-bug-fix 109]
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sun 17-Jul-05 13:19 by teresang

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: ME3400 Boot Loader (me3400-HBOOT-M), Version 12.2 [mbutts-meap2 103]

 tandoori_1 uptime is 1 day, 2 hours, 49 minutes
System returned to ROM by power-on
System image file is "flash:image"

cisco ME-3440-24T-FA (PowerPC405) processor with 118784K/12280K bytes of memory.

Processor board ID FSJC0407862
Last reset from power-on
Target IOS Version 12.2(25)SE
3 Virtual Ethernet interfaces
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
```

```
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0B:FC:FF:32:80
Power supply part number        : 341-0149-01
Motherboard serial number       : FHH0848001R
Power supply serial number      : DTH0450000T
System serial number            : FSJC0407862
Top Assembly Part Number        : 800-26552-01
Top Assembly Revision Number    : 05
Hardware Board Revision Number  : 0x01


Switch   Ports  Model              SW Version              SW Image
------   -----  -----              ----------              ----------
*    1   26     ME-3440-24T-FA     12.2(20050712:084347)   MEAP-IPSERVICES-M


Configuration register is 0xF
```

show vlan

Use the **show vlan** user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

show vlan [**access-map** | **brief** | **dot1q tag native** | **filter** | **id** *vlan-id* | **internal usage** | **mtu** | **name** *vlan-name* | **private-vlan [type]** | **remote-span** | **summary** | **uni-vlan [type]**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

access-map	See the **show vlan access-map** command.
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.. This keyword is supported only when the switch is running the metro IP access or metro access image.
filter	See the **show vlan filter** command.
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). You cannot create VLANs with these IDS by using the **vlan** global configuration command until you remove them from internal use. This keyword is supported only when the switch is running the metro IP access image.
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 [type]	(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. Enter **type** (optional) to see only the VLAN ID and the type of private VLAN.
remote-span	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Display VLAN summary information.
uni-vlan [type]	(Optional) Display user network interface (UNI) VLAN information. Enter **type** (optional) to see only the VLAN ID and type of UNI 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.

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(25)EX	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. 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 a switch virtual interface (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 *normal* type means a VLAN 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 but do not remove 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*.

In the **show vlan uni-vlan type** command output, type is either *community* or *isolated*. User network interfaces (UNIs) in a UNI community VLAN can communicate with each other; UNIs in a UNI isolated VLAN cannot communicate. Network node interfaces (NNIs) can communicate with each other and with UNIs in UNI isolated and community 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 vlan** command. Table 2-19 describes the fields in the display.

Note The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not supported or used.

```
Switch> show vlan
Switch#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

```
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005    1500  -     -     -      ibm  -      0     0VLAN Name

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

VLAN Type              Ports
---------- ----------------- ----------------------------------------
```

Table 2-19 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 configured private VLANs, including the primary VLAN ID, the secondary VLAN ID, the type of secondary VLAN (community or isolated), and the ports that belong to it.
VLAN Type/Ports	Displays any configured UNI VLANs, the type (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          Gi0/3
10      502       community         Fa0/11
10      503       non-operational3      -
20       25       isolated          Fa0/13, Fa0/20, Fa0/22, Gi0/1,
20       30       community         Fa0/13, Fa0/20, Fa0/21, Gi0/1,
20       35       community         Fa0/13, Fa0/20, Fa0/23, Fa0/33. Gi0/1,
20       55       non-operational
2000   2500       isolated          Fa0/5, Fa0/10, Fa0/15
```

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 uni-vlan type** command:

```
Switch> show vlan uni-vlan type
Vlan Type
---- -----------------
1    UNI isolated
20   UNI community
201  UNI isolated
```

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      : 0
 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
---- -------------------------------- --------- -------------------------------

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled
```

This is an example of output from the **show vlan internal usage** command. It shows that VLANs 1025 and 1026 are being used as internal VLANs for Fast Ethernet routed ports 23 and 24. If you want to use one of these VLAN IDs, you must first shut down the routed port, which releases the internal VLAN, and then create the extended-range VLAN. When you start up the routed port, another internal VLAN number is assigned to it.

```
Switch> show vlan internal usage
VLAN Usage
---- -------------
1025 FastEthernet0/23
1026 FastEthernet0/24
```

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	Enables VLAN configuration mode where you can configure VLANs 1 to 4094.

show vlan access-map

Use the **show vlan access-map** privileged EXEC command to display information about a particular VLAN access map or for all VLAN access maps.

show vlan access-map [*mapname*] [| {**begin** | **exclude** | **include**} *expression*]

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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch# show vlan access-map
Vlan access-map "SecWiz"  10
  Match clauses:
    ip  address: SecWiz_Fa1_0_3_in_ip
  Action:
    forward
```

Related Commands

Command	Description
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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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(25)EX	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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. 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 2-20 describes each field in the display.

Table 2-20 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 VQP 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.