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 co	ollection is disabled.
Command Modes	Interface configuration	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	interface (UNI) or enha configuration command	ollection command is based on hardware counters. If the port is a user network nced network interface (ENI), you must use the no shutdown interface to enable it before using the rmon collection stats command. UNIs and ENIs
-	interface (UNI) or enha configuration command are disabled by default.	nced network interface (ENI), you must use the no shutdown interface to enable it before using the rmon collection stats command. UNIs and ENIs Network node interfaces (NNIs) are enabled by default.
-	interface (UNI) or enha configuration command are disabled by default. This example shows ho	nced network interface (ENI), you must use the no shutdown interface to enable it before using the rmon collection stats command. UNIs and ENIs Network node interfaces (NNIs) are enabled by default. w to collect RMON statistics for the owner <i>root</i> :
-	interface (UNI) or enha configuration command are disabled by default. This example shows ho Switch(config)# inter	nced network interface (ENI), you must use the no shutdown interface to enable it before using the rmon collection stats command. UNIs and ENIs Network node interfaces (NNIs) are enabled by default.
-	interface (UNI) or enha configuration command are disabled by default. This example shows ho Switch(config)# inter Switch(config-if)# m	nced network interface (ENI), you must use the no shutdown interface to enable it before using the rmon collection stats command. UNIs and ENIs Network node interfaces (NNIs) are enabled by default. w to collect RMON statistics for the owner <i>root</i> : fface gigabitethernet0/1
Examples	interface (UNI) or enha configuration command are disabled by default. This example shows ho Switch(config)# inter Switch(config-if)# m	nced network interface (ENI), you must use the no shutdown interface to enable it before using the rmon collection stats command. UNIs and ENIs Network node interfaces (NNIs) are enabled by default. w to collect RMON statistics for the owner <i>root</i> : fface gigabitethernet0/1 non collection stats 2 owner root
Usage Guidelines Examples Related Commands	interface (UNI) or enha configuration command are disabled by default. This example shows ho Switch(config)# inter Switch(config-if)# rm You can verify your set	nced network interface (ENI), you must use the no shutdown interface to enable it before using the rmon collection stats command. UNIs and ENIs Network node interfaces (NNIs) are enabled by default. w to collect RMON statistics for the owner <i>root</i> : face gigabitethernet0/1 non collection stats 2 owner root ting by entering the show rmon statistics privileged EXEC command.

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

L

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.

Г

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 orignore the statistics the	command-line help strings, the history keyword is not supported, and you should at it gathers.
Defaults	No policy maps are at	tached to the port.
Command Modes	Interface configuration	n
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: Configurati configurations e	ion failed. Maximum number of allowable unique queue-limit exceeded.
	-	r output policy maps to a Fast Ethernet or Gigabit Ethernet port. You cannot attach virtual interfaces (SVIs) and EtherChannel interfaces.

ExamplesThis example shows how to apply plcmap1 as an output policy map:
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output plcmap1This 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 Displays policy maps configured on the specified interface or on all **interface** [*interface-id*] 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.

Γ

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 output 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 ar	e defined.
Command Modes	Policy-map class conf	iguration
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	creates hierarchical po	blicy created in policy-map class configuration to a parent output policy map. This blicy mapping. Use the service-policy <i>policy-map-name</i> policy-map class and to enter a second-level (child) policy map.
	configure hierarchical the class class-defaul port and is the parent by using the queue-li	nap, when shape average is also configured on the class class-default , you can policy maps by attaching a single service-policy policy-map class command to t . This policy map specifies the service policy for the port-shaped traffic on the policy map. You can configure the child policy with class-based queuing actions mit policy map class command and with scheduling actions (by using the erage , or priority command).
	-	p configuration mode, use the exit command. To return to privileged EXEC mode,
Examples	-	now to define the service policy and to attach it to a parent policy map to set the (shape) for an output queue at 90000000 bits per second:
	Switch(config)# pol Switch(config-pmap) Switch(config-pmap-	<pre>icy-map out-policy-parent # class class-default c)# shape average 90000000 c)# service-policy out-policy c)# exit</pre>
	You can verify your se	ettings 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 <i>map-from</i> 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 <i>from-field</i> 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	s defined.
Command Modes	Policy-map class co	nfiguration
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		
Usage Guidennes	qos-group, for the sa	et cos with all other marking actions, specifically set dscp, set precedence, and set ame class. Support was also added for the ability to configure more than one marking d packet marking by using table maps for the same class.
		mand if you want to mark a packet that is being sent to a switch. Switches can ader 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.

Γ

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*]}



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 <i>map-from</i> 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 <i>from-field</i> 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	n	

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	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 <i>dscp-value</i> by using the reserved keywords EF , AF11 , and AF12 .			
	If you are using this command to perform enhanced packet marking, you can use the <i>from-field</i> packet marking option for mapping and setting the DSCP value. The supported <i>from-field</i> marking categories are: CoS, DSCP, and IP precedence.			
	If you specify a <i>from-field</i> category, but do not specify the table keyword and <i>table-map-name</i> , the default action is to copy the value associated with the <i>from-field</i> 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:			
	<pre>Switch(config)# policy-map policy_ftp Switch(config-pmap)# class ftp_class Switch(config-pmap-c)# set dscp 10 Switch(config-pmap-c)# exit</pre>			
	This example shows how to assign a CoS to DSCP table map to a class:			
	<pre>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</pre>			
	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*]}



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 <i>map-from</i> 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 <i>from-field</i> 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 con	figuration
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 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 co	onfiguration
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	precedence , for the marking action with	set qos-group with all other marking actions, specifically set cos, set dscp, and set e same class. Support was also added for the ability to configure more than one n enhanced packet marking by using table maps for the same class.
		to associate a QoS group value with a traffic flow as it enters the switch, which can butput policy map to identify the flow.
	A maximum of 100	QoS groups (0 through 99) is supported on the switch.
	To return to policy- use the end comma	map configuration mode, use the exit command. To return to privileged EXEC mode, nd.
Examples	This example shows	s how to set all FTP traffic to QoS group 5:
	Switch(config-pma	olicy-map policy_ftp p)# class ftp_class p-c)# set qos-group 5 p-c)# exit
	You can verify your	r 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 1 no ip routing ! interface GigabitEthernet0/1 no ip address interface GigabitEthernet0/2 no ip address 1 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_co mmand_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 or port 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 100000000 for class-based shaping and 4000000 to 1000000000 for port shaping.
Defaults	No traffic shaping i	s defined.
Command Modes	Policy-map class co	onfiguration
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.
	class or class-defau Configuring traffic	its the rate of transmission of data. Configuring traffic shaping for a user-defined alt for class-based shaping sets the peak information rate (PIR) for that class. shaping for the class class-default when it is the only class in the policy map that is face sets the PIR for the interface (port shaping).
		re shape average in a class that includes priority queueing (configured with the p class configuration command).
		command uses a default queue limit for the class. You can change the queue limit by hit policy-map class command, overriding the default that is set by the shape average
		bandwidth policy-map class configuration command to configure class-based ng (CBWFQ) and the shape average command to configure traffic shaping for the
		nierarchical policy maps by attaching the service-policy policy-map class command efault only when shape average is also configured on the class class-default .

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-c)# shape average 20000000
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# 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.
	<pre>show policy-map interface [interface-id]</pre>	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.
	ірс	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	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 or 1 to 199 and 1300 to 2	nly IP standard and extended access lists. Therefore, the allowed numbers are only 699.
	-	ensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> the lines that contain <i>Output</i> 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 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
                        All frame count: 0
     Drop And Log:
     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
                         All bytes count: 0
     Bridge Only:
     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
                        All bytes count: 1236182
     Forwarded:
     Forwarded And Log: All frame count: 0
     Forwarded And Log: All bytes count: 0
 L2 ACL OUTPUT Statistics
              All frame count: 0
     Drop:
     Drop:
                         All bytes count: 0
                     All frame count: 0
     Drop And Log:
     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
                        All frame count: 0
     Drop:
     Drop:
                         All bytes count: 0
                         All frame count: 0
     Drop And Log:
     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:	A11	bytes	count:	0
Forwarding To CPU:	A11	frame	count:	0
Forwarding To CPU:	A11	bytes	count:	0
Forwarded:	A11	frame	count:	514434
Forwarded:	A11	bytes	count:	39048748
Forwarded And Log:	A11	frame	count:	0
Forwarded And Log:	A11	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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified expression.
	expression	Expression in the output to use as a reference point.
Command Modes	Privileged EX	KEC
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	•	archive download-sw privileged EXEC command to download an image to a TFTP server, the show archive status command shows the status of the download.
	-	are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> ayed, but the lines that contain <i>Output</i> are displayed.
Examples	These are exa	amples of output from the show archive status command:
		v archive status grade in progress
		v archive status grade in progress
		v archive status cracting the image
		v archive status Lfying software
		v archive status rade completed. Reload pending
Related Commands	Command	Description
	archive dow	nload-sw Downloads a new image from a TFTP server to the switch.

show arp access-list

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

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

Syntax Description		
eynax Decemption	acl-name (C	Optional) Name of the ACL.
	l begin (C	Optional) Display begins with the line that matches the <i>expression</i> .
	exclude (C	Optional) Display excludes lines that match the <i>expression</i> .
	include (C	Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i> Ex	xpression in the output to use as a reference point.
Command Modes	User EXEC	
Command History	Release	Modification
	12.2(50)SE	This command was introduced.
	are not displayed,	ase sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> , but the lines that contain <i>Output</i> are displayed.
Examples		, but the lines that contain <i>Output</i> are displayed.
Examples	This is an exampl	, but the lines that contain <i>Output</i> are displayed. le of output from the show arp access-list command:
Examples		, but the lines that contain <i>Output</i> are displayed. le of output from the show arp access-list command: p access-list
Examples	This is an exampl Switch> show arg ARP access list permit ip 10	, but the lines that contain <i>Output</i> are displayed. le of output from the show arp access-list command: p access-list
	This is an exampl Switch> show arg ARP access list permit ip 10 permit ip 20	, but the lines that contain <i>Output</i> are displayed. le of output from the show arp access-list command: p access-list rose 0.101.1.1 0.0.0.255 mac any 0.3.1.0 0.0.0.255 mac any
	This is an exampl Switch> show arg ARP access list permit ip 10 permit ip 20 Command	, but the lines that contain <i>Output</i> are displayed. le of output from the show arp access-list command: p access-list rose 0.101.1.1 0.0.0.255 mac any 0.3.1.0 0.0.0.255 mac any Description
Examples Related Commands	This is an exampl Switch> show arg ARP access list permit ip 10 permit ip 20 Command arp access-list	, but the lines that contain <i>Output</i> are displayed. le of output from the show arp access-list command: p access-list rose 0.101.1.1 0.0.0.255 mac any 0.3.1.0 0.0.0.255 mac any Description Defines an ARP ACL.
	This is an exampl Switch> show arg ARP access list permit ip 10 permit ip 20 Command	, but the lines that contain <i>Output</i> are displayed. le of output from the show arp access-list command: p access-list rose 0.101.1.1 0.0.0.255 mac any 0.3.1.0 0.0.0.255 mac any Description Defines an ARP ACL.
	This is an exampl Switch> show arp ARP access list permit ip 10 permit ip 20 Command arp access-list deny (ARP access	, but the lines that contain <i>Output</i> are displayed. le of output from the show arp access-list command: p access-list rose 0.101.1.1 0.0.0.255 mac any 0.3.1.0 0.0.0.255 mac any Description Defines an ARP ACL. ss-list Denies an ARP packet based on matches against the Dynamic Host Configuration Protocol (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 <i>expression</i> .
	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
	10.0(05) EX	
Hoogo Guidolingo	12.2(25)EX	This command was introduced.
Usage Guidelines	Expressions are case are not displayed, bu	sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> t the lines that contain <i>Output</i> are displayed.
Usage Guidelines Examples	Expressions are case are not displayed, bu	sensitive. For example, if you enter exclude output , the lines that contain <i>output</i>

Table 2-4 describes each field in the display.

Field	Description
BOOT path-list	Displays a semicolon separated list of executable files to try to load and execute when automatically booting.
	If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.
	If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to no or 0, the boot loader attempts to automatically boot 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*]

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

d Description	interface-id	Specify the interface on which TDR was run.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified 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 a Cisco ME switch:	This is an example of output from the show cable-diagnostics tdr interface <i>interface-id</i> command on a Cisco ME switch:				
	Switch# show cable-diagnostics tdr interfac TDR test last run on: March 01 18:14:44	e fastethernet0/1				
	Interface Speed Local pair Pair length	Remote pair Pair status				

Fa0/1	100M	Pair	A	4	+/- 5	5	meters	Pair	A	Normal
		Pair	В	4	+/- 5	5	meters	Pair	В	Normal
		Pair	С	N/A				Pair	С	N/A
		Pair	D	N/A				Pair	D	N/A

Table 2-5 lists the descriptions of the fields in 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.					
	• ImpedanceMis—The impedance is mismatched.					
	• Short/Impedance Mismatched—The impedance mismatched or the cable is short.					
	• InProgress—The diagnostic test is in progress					

 Table 2-5
 Fields Descriptions for the show cable-diagnostics tdr Command Output

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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	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	e of output from the show class-map command:
Examples	-	
	_	ss-map all videowizard_10-10-10 (id 2) group name videowizard_10-10-10
	Match any	-any class-default (id 0) -all dscp5 (id 3) 5
Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.

Defines the match criteria to classify traffic.

match access-group

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 <i>expression</i> .						
	exclude	(Optional)	Display exc	cludes lines t	that match the ex	pression.	
	include	(Optional) Display includes lines that match the specified <i>expression</i> .					
	expression	Expression	in the outp	out to use as	a reference point	•	
Command Modes	Privileged EXEC						
Command History	Release	Modif	ication				
	12.2(25)EX	This c	command w	as introduce	d.		
	troubleshooting the						
Examples	Expressions are cas are not displayed, t This is a partial out	e sensitive. Fout the lines t put the lines t	hat contain from the sh	<i>Output</i> are d	lisplayed.		-
xamples	Expressions are cas are not displayed, b This is a partial out Switch# show cont cpu-queue-frames	se sensitive. Fout the lines t put example cput example crollers cpu retrieved	hat contain from the sh -interface dropped	Output are d	lisplayed.		-
xamples	Expressions are cas are not displayed, b This is a partial out Switch# show cont cpu-queue-frames	se sensitive. F out the lines t put example crollers cpu	hat contain from the sh -interface dropped	Output are d	lisplayed. ers cpu-interfac		-
xamples	Expressions are cas are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t put example crollers cpu retrieved 4523063 1545035 1903047	hat contain from the sh -interface dropped 0 0 0	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0		-
xamples	Expressions are cas are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t put example crollers cpu retrieved 4523063 1545035 1903047 96145	hat contain from the sh -interface dropped 0 0 0 0	Output are d now controll invalid 0 0 0 0	lisplayed. ers cpu-interfac hol-block 0 0 0 0		-
xamples	Expressions are cas are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t eput example crollers cpu retrieved 4523063 1545035 1903047 96145 79596	hat contain from the sh -interface dropped 0 0 0 0 0 0	Output are d now controll invalid 0 0 0 0 0	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cas are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t put example crollers cpu retrieved 4523063 1545035 1903047 96145 79596 0	hat contain from the sh -interface dropped 0 0 0 0 0 0 0 0 0	Output are d	lisplayed. ers cpu-interfac hol-block - 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cass are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t eput example crollers cpu retrieved 4523063 1545035 1903047 96145 79596 0 5756	hat contain from the sh -interface dropped 0 0 0 0 0 0	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cass are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t eput example crollers cpu retrieved 4523063 1545035 1903047 96145 79596 0 5756 225646	hat contain from the sh -interface dropped 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cass are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t eput example crollers cpu retrieved 4523063 1545035 1903047 96145 79596 0 5756	hat contain from the sh -interface dropped 0 0 0 0 0 0 0 0 0 0 0 0 0	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cass are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t put example retrieved 4523063 1545035 1903047 96145 79596 0 5756 225646 46472	hat contain from the sh -interface dropped 	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cass are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t put example retrieved 	hat contain from the sh -interface dropped 	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cass are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t put the lines t rollers cpu retrieved 4523063 1545035 1903047 96145 79596 0 5756 225646 46472 0 68411	hat contain from the sh -interface dropped 	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cass are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t put the lines t rollers cpu retrieved 	hat contain from the sh -interface dropped 	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 0 0 0		-
xamples	Expressions are cass are not displayed, b This is a partial out Switch# show cont cpu-queue-frames 	e sensitive. Fout the lines t cput example retrieved 	hat contain from the sh -interface dropped 	Output are d	lisplayed. ers cpu-interfac hol-block 0 0 0 0 0 0 0 0 0 0 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 80000800 MicDirectPollInfo MicIndicationsReceived 00000000 00000000 MicInterruptsReceived MicPcsInfo 0001001F 00000000 MicPlbMasterConfiguration 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 Fifo_Flag: 89800400 WritePtrs: 03A9BC60 writeHeaderPtr: 03A9BC60 038C8800 038C88E0 Fifo2: StartPtr: ReadPtr: 038C88E0 88800200 WritePtrs: Fifo_Flag: 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 88800200 WritePtrs: 03A7A600 Fifo_Flag: 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).
Syntax Description		
	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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified expression.
	expression	Expression in the output to use as a reference point.
Command Modes		(only supported with the <i>interface-id</i> 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.	
	•	he phy or port-asic keywords, the displayed information is useful primarily for Cisco representatives troubleshooting the switch.
	11	

Transmi

Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface. Table 2-6 describes the *Transmit* fields, and Table 2-7 describes the *Receive* fields.

Switch# show controllers ethernet-controller gigabitethernet0/1

‡ £	show controllers ethernet-contr	roller gigabitethernet0/1
Lt	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 2-6 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.

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.

	Table 2-6	Transmit Field Descriptions (continued)
--	-----------	-----------------------------------------

1. CFI = Canonical Format Indicator

Table 2-7 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.

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 2-7 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.

Switch# show controllong othernot controllon significations (0/2 nhw

Table 2-7 Receive Field Descriptions (continued)

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-c	ontrol	ller gi	.gabit	tethei	net0/2	phy
Control Register	:	0001 0	001 (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	[Adm:	inStat	ce=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 : 00000000 Reset PmadMicConfig : 00000001 PmadMicDiag : 0000003 : 000007D0 000007D0 40000000 : 000001D0 000001D0 40000000 SupervisorReceiveFifoSramInfo SupervisorTransmitFifoSramInfo 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	0000003	7F001644	0000003
		24140003	FD632B00	18E418E0	FFFFFFFF
StackControlStatus	:	18E418E0			
stackControlStatusMask	:	FFFFFFF			
TransmitBufferFreeListInfo	:	00000854	00000800	00000FF8	00000000
		0000088A	0000085D	00000FF8	00000000
TransmitRingFifoInfo	:	00000016	00000016	4000000	00000000
		0000000C	0000000C	4000000	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	0000001	0EC0801B	0000001
		00C0001D	0000001	00C0001E	0000001

<output truncated>

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

_____ PortASIC 0 Statistics _____ 0 RxQ-0, wt-0 enqueue frames0 RxQ-0, wt-0 drop frames66 RxQ-0, wt-1 enqueue frames0 RxQ-0, wt-1 drop frames 4118966 RxQ-0, wt-1 enqueue frames 0 RxQ-0, wt-2 enqueue frames 0 RxQ-0, wt-2 drop frames 0 RxQ-1, wt-0 drop frames 0 RxQ-1, wt-0 enqueue 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 0 RxQ-2, wt-2 drop frames 158377 RxQ-2, wt-2 enqueue frames 0 RxQ-3, wt-0 enqueue frames 0 RxQ-3, wt-0 drop frames 0 RxQ-3, wt-1 drop frames 0 RxQ-3, wt-1 enqueue 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 0 Rx Too Old Frames 74 RxBuffer Drop DestIndex Cou 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

Switch# show controllers ethernet-controller port-asic statistics

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 drop frames
52 RxQ-0, wt-1 enqueue frames 0 RxQ-0, wt-2 enqueue frames	0 RxQ-0, wt-1 drop 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							
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 <i>expression</i> .					
	l exclude (Optional) Display excludes lines that match the <i>expression</i> .						
	include	(Optional) Display includes lines that match the specified expression.					
	expression	Expression in the output to use as a reference point.					
Command Modes	Privileged EX	EC					
Command History	Release	Modification					
	12.2(25)EX	This command was introduced.					
Examples		but the lines that contain <i>Output</i> appear. mple of output from the show controllers tcam command:					
	Switch# show controllers tcam						
	TCAM-0 Regis	lers					
	REV: 001 SIZE: 00 ID: 00	ters 330103 080040 000000 000000_F0000020					
	REV: 001 SIZE: 000 ID: 000 CCR: 000 RPID0: 000 RPID1: 000 RPID1: 000	B30103 080040 000000					

```
HRR3: 0000000_0000000
 HRR4: 00000000_0000000
 HRR5: 0000000_0000000
 HRR6: 0000000_0000000
 HRR7: 00000000_0000000
<output truncated>
 GMR31: FF_FFFFFFFFFFFFFFFFF
 ______
TCAM related PortASIC 1 registers
LookupType:
                   89A1C67D_24E35F00
LastCamIndex:
                    0000FFE0
LocalNoMatch:
                    000069E0
ForwardingRamBaseAddress:
                    00022A00 0002FE00 00040600 0002FE00 0000D400
                    00000000 003FBA00 00009000 00009000 00040600
                    0000000 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) II	O of the switch interface.			
	begin	(Optional) D	isplay begins with the line that matches the specified <i>expression</i> .			
	exclude	(Optional) D	isplay excludes lines that match the specified <i>expression</i> .			
	include	(Optional) D	isplay includes lines that match the specified <i>expression</i> .			
	expression	Expression in	n the output to use as a reference point.			
Command Modes	User EXEC					
Command History	Release	N	lodification			
	12.2(25)EX	Т	his command was introduced.			
Examples			from the show controllers utilization command.			
	Switch> show controllers utilization					
	Port R Fa0/1	eceive Utiliza O	tion Transmit Utilization 0			
	Fa0/1 Fa0/2	0	0			
	Fa0/3	0	0			
	Fa0/4	0	0			
	Fa0/5	0	0			
	Fa0/6 Fa0/7	0 0	0 0			
	<output truncated=""></output>					
	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:					
	Receive Band	width Percenta	<pre>igabitethernet0/1 utilization ge Utilization : 0 age Utilization : 0</pre>			

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.

Table 2-8 show controllers utilization Field Descriptions

Related Commands

Command	Description
show controllers ethernet-controller	Displays the interface internal registers.
culturer controller	

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 ture, module, and port number)				
	atatistica intenface	type, module, and port number).				
	statistics interface(Optional) Display IEEE 802.1x statistics for the specified portinterface-idtype, module, and port number).					
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .				
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .				
	I include (Optional) Display includes lines that match the specified <i>expression</i> .					
	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.				
	-	nsitive. For example, if you enter exclude output , the lines that contain <i>output</i> ne lines that contain <i>Output</i> appear.				
Examples	_	utput from the show dot1x and the show dot1x all privileged EXEC commands:				
	Switch# show dot1x Sysauthcontrol Dot1x Protocol Versic Dot1x Oper Controlled Dot1x Admin Controlled	d Directions = Both				
	Switch# show dot1x al Dot1x Info for interf	L1 face GigabitEthernet0/1				
	PortStatus = U MaxReq = 2 HostMode = 5	= CONNECTING = IDLE JNAUTHORIZED				

Cisco ME 2400 Ethernet Access Switch Command Reference

QuietPeriod	= 60 Seconds
Re-authentication	= Disabled
ReAuthPeriod	= 3600 Seconds
ServerTimeout	= 30 Seconds
SuppTimeout	= 30 Seconds
TxPeriod	= 30 Seconds
Guest-Vlan	= 0
Dot1x Info for int	terface GigabitEthernet0/2
PortStatus	= UNAUTHORIZED
MaxReq	= 2
HostMode	= Multi
Port Control	= Auto
QuietPeriod	= 60 Seconds
Re-authentication	= Disabled
ReAuthPeriod	= 3600 Seconds
ServerTimeout	= 30 Seconds
	50 50001145
SuppTimeout	

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

Supplicant MAC 0000.D/1D.350e				
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 2-9 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 2-9show 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.		

Field	Description		
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.		

Table 2-9 show dot1x statistics Field Descriptions (continued)

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, and power information for the switch.

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

Although visible in the command-line interface, the **status** keyword is not supported.

Syntax Description	all	Display both fan and temperature environmental status.				
Syntax Description	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	ture Display the switch temperature status as OK or FAULTY.				
	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 History	Release 12.2(25)EX	Modification This command was introduced.				
Command History Usage Guidelines	12.2(25)EX Expressions are c	This command was introduced. ease sensitive. For example, if you enter exclude output , the lines that contain <i>outpu</i>				
	12.2(25)EX Expressions are c	This command was introduced.				
	12.2(25)EX Expressions are c are not displayed	This command was introduced. ease sensitive. For example, if you enter exclude output , the lines that contain <i>outpu</i>				
Usage Guidelines	12.2(25)EX Expressions are c are not displayed	This command was introduced. This command was introduced. This command was introduced. This commander is a second command of the second command command of the second command command of the second command comma				
Usage Guidelines	12.2(25)EX Expressions are c are not displayed This is an examp Switch# show en FAN is OK TEMPERATURE is POWER is OK RPS is NOT PRES	This command was introduced. This command was introduced. This command was introduced. This commander is a set of the				

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 (C	Optional) Display begins with the line that matches the <i>expression</i> .
	exclude (C	Optional) Display excludes lines that match the <i>expression</i> .
	include (0	Optional) Display includes lines that match the specified <i>expression</i> .
		xpression 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 ph	nysical port is error disabled if a violation occurs.
	• vlan—The vi	rtual port is disabled if a violation occurs.
	• port/vlan—S	ome ports are configured for physical port disable, and others are configured for virtual Enter the show running config privileged EXEC command to see the configuration for
	_	-invalid error in the Reason column refers to an invalid small form-factor pluggable
	_	ase sensitive. For example, if you enter I exclude output , the lines that contain <i>output</i> , but the lines that contain <i>Output</i> are displayed.
Examples	This is an examp	le of output from the show errdisable detect command:
	Switch> show er ErrDisable Reas	on Detection Mode
	arp-inspection bpduguard channel-misconf	Enabled port Enabled port
	community-limit dhcp-rate-limit dtp-flap	-
	gbic-invalid	Enabled port
	invalid-policy	Enabled port
	12ptguard	Enabled port
	link-flap	Enabled port

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

Note

Though visible in the output, the dtp-flap, l2ptguard, ilpower, storm-control, arp-inspection, 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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	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	will cause an will be assum access/trunk)	umn in the display shows how many changes to the state within the specified time interval error to be detected and a port to be disabled. For example, the display shows that an error red and the port shut down if three Dynamic Trunking Protocol (DTP)-state (port mode or Port Aggregation Protocol (PAgP) flap changes occur during a 30-second interval, or if ink up/down) changes occur during a 10-second interval.
	ErrDisable F	
	pagp-flap dtp-flap link-flap	3 30 3 30 5 10
Note	Although visi	ble in the output display, the switch does not support DTP.
	-	are case sensitive. For example, if you enter I exclude output , the lines that contain <i>output</i> yed, but the lines that contain <i>Output</i> are displayed.
Examples	This is an exa	mple of output from the show errdisable flap-values command:
	ErrDisable F	
	pagp-flap dtp-flap	3 30 3 30

Related Commands 0

ommands	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]

begin (C	Optional) Display begins with the line that matches the <i>expression</i> .
exclude (0	Optional) Display excludes lines that match the <i>expression</i> .
include (0	Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i> E	xpression in the output to use as a reference point.
User EXEC	
Release	Modification
12.2(25)EX	This command was introduced.
-	case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> , but the lines that contain <i>Output</i> are displayed.
A gbic-invalid er interface.	cror-disable reason refers to an invalid small form-factor pluggable (SFP) module
This is an examp	le of output from the show errdisable recovery command:
Switch> show er	rdisable recovery
ErrDisable Reas	
udld	Disabled
bpduguard	Disabled
security-violat	io Disabled
channel-misconf	
-	Disabled
	Disabled
	Disabled
-	Enabled on Disabled
-	Disabled
-	
-	Disabled
	Disabled
	Disabled
loopback	Disabled
	I exclude (0 I include (0 I include (0 I include (0 expression E User EXEC Expressions are of are not displayed A gbic-invalid er interface. Interface. This is an examp Switch> show er Switch> show er ErrDisable Reas udld bpduguard security-violat Security-violat

Interface Errdisable reason Time left(sec)

Interiace	Errdisable reason	Time left(sec)
Gi0/2	link-flap	279



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 <i>expression</i> .					
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .(Optional) Display includes lines that match the specified <i>expression</i> .					
	include						
	<i>expression</i> 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 <i>cl</i>	nannel-group, all channel groups are displayed.					
	Expressions are case sense	sitive. 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 = Pol
                       Load = 0x00
                                         Protocol = LACP
Port index
          = 0
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
                                                      Number State
        Flags State
Port.
                        Priority
                                     Key
                                              Key
Gi0/1
              bndl
                        32768
                                                              0x3D
       SA
                                     0 \ge 0
                                              0x1
                                                      0 \ge 0
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 LACP Gi0/1(P) Gi0/2(P) 1 Pol(SU) 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: EC state No of bits Index Load Port 0 00 Gi0/1 Active 0 0 00 Gi0/2 Active 0 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 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	(Option interface		ay the flow c	ontrol stat	tus and statistics for a specific	
	module number	switch.	(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	(Option	al) Displ	ay begins wit	h the line	that matches the <i>expression</i> .	
	exclude	(Option	al) Displ	ay excludes 1	ines that r	natch the <i>expression</i> .	
	I include (Optional) Display includes lines that match the specified <i>expression</i> .						
	expression	Express	ion in the	e output to us	e as a refe	erence point.	
Command Modes	User EXEC						
Command History	Release	Modific	ation				
	12.2(25)EX	This co	mmand w	as introduce	1.		
Usage Guidelines	Use the show flowcont from the show flowcon <i>number</i> command.	rol comma trol comm	nd to dis and is the	play informates a same as the	tion about output fro	n the switch or for a specific interface. all the switch interfaces. The output om the show flowcontrol module play information about a specific	
	interface.						
	Expressions are case se do not appear, but the l		-	•	exclude	e output, the lines that contain <i>output</i>	
Examples	This is an example of o	utput from	the show	v flowcontro	l comman	d.	
	admin	Control R oper a	ıdmin	FlowControl oper			
	Gi0/1 Unsupp. 1 Gi0/2 desired of Gi0/3 desired of	Jnsupp. c		off off off	0 0 0	 0 0 0	
	<output truncated=""></output>						

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

Switch> sh	ow flowco	ntrol int	erface gi	gabitetherne	t0/2	
Port	Send Flo	wControl	Receive	FlowControl	RxPause	TxPause
	admin	oper	admin	oper		
Gi0/2	desired	off	off	off	0	0

ls	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 <i>expression</i> .			
	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	in the SFP module slot. Expressions are case sen	only to Gigabit Ethernet interfaces and displays information about SFPs inserted nsitive. For example, if you enter I exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear.			
	in the SFP module slot. Expressions are case sen do not appear, but the lin	nsitive. For example, if you enter I exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear.			
Usage Guidelines Examples	in the SFP module slot. Expressions are case sen do not appear, but the lin This is an example of our	nsitive. For example, if you enter l exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear. tput from the show idprom interface command for a Gigabit Ethernet interface			
	in the SFP module slot. Expressions are case sen do not appear, but the lin This is an example of our	nsitive. For example, if you enter I exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear.			
	in the SFP module slot. Expressions are case sen do not appear, but the lin This is an example of our	nsitive. For example, if you enter l exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 on			
	in the SFP module slot. Expressions are case sen do not appear, but the lin This is an example of our Switch # show idprom i General SFP Informati 	<pre>nsitive. For example, if you enter l exclude output, the lines that contain output nes that contain Output appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 .on </pre>			
	in the SFP module slot. Expressions are case sen do not appear, but the lin This is an example of our Switch# show idprom in General SFP Informati Identifier Connector Transceiver	histive. For example, if you enter l exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 on : 0x03 : 0x07 : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x			
	in the SFP module slot. Expressions are case sen do not appear, but the lin This is an example of our Switch # show idprom i General SFP Informati 	<pre>nsitive. For example, if you enter exclude output, the lines that contain output nes that contain Output appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 .on </pre>			
	in the SFP module slot. Expressions are case sendo not appear, but the line This is an example of our Switch# show idprom in General SFP Informati 	nsitive. For example, if you enter l exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 .on 			
	in the SFP module slot. Expressions are case sendo not appear, but the line This is an example of our Switch# show idprom in General SFP Informati 	nsitive. For example, if you enter l exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 .on 			
	in the SFP module slot. Expressions are case sendo not appear, but the line This is an example of our Switch# show idprom is General SFP Informati 	nsitive. For example, if you enter exclude output, the lines that contain output nes that contain Output appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 .on 			
	in the SFP module slot. Expressions are case sendo not appear, but the line This is an example of our Switch# show idprom is General SFP Informati Identifier Connector Transceiver Encoding BR_Nominal Vendor Name Vendor Part Number Vendor Revision Vendor Serial Number Other Information	nsitive. For example, if you enter exclude output, the lines that contain <i>output</i> nes that contain <i>Output</i> appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 on 			
	in the SFP module slot. Expressions are case sendo not appear, but the line This is an example of our Switch# show idprom is General SFP Informati Identifier Connector Transceiver Encoding BR_Nominal Vendor Name Vendor Part Number Vendor Revision Vendor Serial Number Other Information	nsitive. For example, if you enter l exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 .on 			
	in the SFP module slot. Expressions are case sendo not appear, but the line This is an example of our Switch# show idprom is General SFP Informati Identifier Connector Transceiver Encoding BR_Nominal Vendor Name Vendor Part Number Vendor Revision Vendor Serial Number Other Information Port asic num Port asic port num	<pre>nsitive. For example, if you enter exclude output, the lines that contain output nes that contain Output appear. tput from the show idprom interface command for a Gigabit Ethernet interface nterface gigabitethernet0/1 on</pre>			

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						
Link Status	: 1					
Link Status Media	: 1					
	: 0					
Resolved Media	: 1					
Config Media	: 1					
	: 0					
Access Count Max	: 2					
Port Rx Loss	: no					
	: no					
Port Tx Disable	: no					
Sfp selection asic re	g map					
stbi	: 0x00					
sfpControl	• 0x4C					
Regs Loc	: 0xF000000					
Page 0 Registers						
0000: 1140 Control R		:				
0001: 6149 Control S	TATUS	:	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-Nego	tiation Advertisement	:	0000	0001	1110	0001
0005: 0000 Auto-Nego	tiation Link Partner	:	0000	0000	0000	0000
0006: 0004 Auto-Nego	tiation Expansion Reg	:	0000	0000	0000	0100
0007: 2001 Next Page		:	0010	0000	0000	0001
	ner Next page Registe				0000	
0009: 0F00 1000BASE-			0000			
000A: 0000 1000BASE-	-	:			0000	
000F: 0000 Extended	5	:	0000			
	fic Control Register		0110	0000	0010	1000
—	fic Status Register		0110			
sorr. sees rur spect		•	5110	TT 00		

0012: 0000 Interrupt Enable Register : 0000 0000 0000 0000 : 0000 0111 0000 0000 0013: 0700 PHY Specific Status Register2 0015: 01C0 Receive Error Counter : 0000 0001 1100 0000 : 0000 0000 0000 0000 0016: 0000 Page Address Register
 0018: 0000 Fage Address Register
 : 0000 0000 0000 0000

 001A: 8040 PHY Specific Control Register2
 : 1000 0000 0100 0000

<output truncated>

Related Commands	Command	Description
	show controllers	Displays per-interface send and receive statistics read from the
	ethernet-controller	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 | stats | status [err-disabled] | switchport
 [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
	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 <i>unsupported</i> 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 port, including port blocking and port protection settings.
	transceiver [detail	(Optional) Display the physical properties of a small form-factor (SFP) module interface. The keywords have these meanings:
	properties]	• 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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified expression.
	expression	Expression in the output to use as a reference point.
	1	L L L L L L L L L L L L L L L L L L L

Note

Though visible in the command-line help strings, the backup, crb, fair-queue, irb, mac-accounting, precedence, private-vlan mapping, 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 1094395 131900022 559555 84077157 IP Spanning Tree 283896 17033760 42 2520 63738 3825680 231 13860 ARP Interface Vlan2 is disabled Vlan7 Pkts In Chars In Pkts Out Chars Out Protocol 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:	modell-ic
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:	<pre>rx-(off,on,desired),tx-(none)</pre>
Fast Start:	yes
QoS scheduling:	<pre>rx-(not configurable on per port basis),tx-(4q2t)</pre>
CoS rewrite:	yes
ToS rewrite:	yes
UDLD:	yes
SPAN: s	ource/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
                                   Connects to Marketing
           up
                          down
```

_ _ _ _

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
                  = 10/1 Number of ports = 0
= 0x00000000 HotStandBy port = null
Logical slot/port = 10/1
GC
                 = Port-channel Ag-Not-Inuse
Port state
Port-channel2:
Age of the Port-channel = 03d:20h:17m:29s
Logical slot/port = 10/2 Number of ports = 0
            = 0x00000000 HotStandBy port = null
GC
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
                 = 0 \times 000000000
                                  HotStandBy port = null
                 = Port-channel Ag-Not-Inuse
Port state
```

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 C	hars In Pkts	Out Cha	rs 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

SWICCH# BHOW II	icerraces statt	15				
Port Name		Status	Vlan	Duplex	Speed	Туре
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 gig	abitethernet0,	/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 2-10 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: dotlq
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: dotlg
```

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 2-10 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	Displays the administrative and operational modes.
Operational Mode	
Administrative Trunking Encapsulation	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Negotiation of Trunking	
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	Displays whether or not unknown multicast and unknown
Unknown multicast blocked	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: Gi0/2
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 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 mode	Configures the VLAN membership mode of a port.
	switchport mode private-vlan	Configures a port as a private-VLAN host or a promiscuous port.
	switchport private-vlan	Defines private-VLAN association for a host port or private-VLAN mapping for a promiscuous port.

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



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

Command Modes Priv

Privileged EXEC

Command History	Release	Мо	odification			
	12.2(25)EX	Th	is command was	s introduced.		
Usage Guidelines	If you do not en	ter any keyw	ords, all counter	s for all interfac	es are included.	
	Expressions are case sensitive. For example, if you enter I exclude output , the lines that contain <i>o</i> are not displayed, but the lines that contain <i>Output</i> are displayed.					lines that contain <i>output</i>
Examples	This is an exam counters for the		output from the	show interface	s counters comma	and. It displays all
	Switch# show i	nterfaces co	ounters			
	Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	
	Fa0/1	0	0	0	0	
	Fa0/2 <output th="" trunca<=""><th>0 .ted></th><th>0</th><th>0</th><th>0</th><th></th></output>	0 .ted>	0	0	0	

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 co	unters 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 <i>expression</i> .		
	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 <i>entity-name</i> keyword was added.		
	(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 a	re not programmed with PIDs and VID.s		
 Note	If there is no PID, no output appears when you enter the show inventory command.			
		o output appears when you enter the show inventory command.		
	-			
Examples	are not displayed, bu	e sensitive. For example, if you enter exclude output , the lines that contain <i>output</i>		
Examples	are not displayed, bu This is example outp Switch> show inver NAME: "1", DESCR:	e sensitive. For example, if you enter I exclude output , the lines that contain <i>output</i> at the lines that contain <i>Output</i> are displayed. put from the show inventory command:		

show ip arp inspection

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

show ip arp inspection [interfaces [interface-id] | log | statistics [vlan vlan-range] | vlan
vlan-range] [| {begin | exclude | include} expression]

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

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.
Examples This is an example of output from the **show ip arp inspection** command

Switch# show ip arp inspection

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

Vlan	Configuration	Operation	ACL Match	Static ACL
1	Enabled	Active	deny-all	No
Vlan	ACL Logging	DHCP Logg	ing Probe 1	Logging
1	Acl-Match	A11	Permit	
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
1	0	0	0	0
Vlan				Source MAC Failures
	0	0	0	0
Vlan	Dest MAC Failures	IP Valid	ation Failures	Invalid Protocol Data
1	0		0	0

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

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

Interface	Trust State	Rate (pps)	Burst Interval
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 gigab	itethernet0/1
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 1	1993					
Gi0/1	5	0001.0000.d774	128.1.9.25	6	DHCP Deny	19:39:02 UTC
Mon Mar 1 1	1993					
Gi0/1	5	0001.c940.1111	10.10.10.1	7	DHCP Deny	19:39:03 UTC
Mon Mar 1 1	1993					
Gi0/1	5	0001.c940.1112	10.10.10.2	8	DHCP Deny	19:39:04 UTC
Mon Mar 1 1	1993					
Gi0/1	5	0001.c940.1114	173.1.1.1	10	DHCP Deny	19:39:06 UTC
Mon Mar 1 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 inspe	ection statis	stics	
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
5	3	4618	4605	4
2000	0	0	0	0
Vlan	DHCP Permits	ACL Permits	Source MAC Fail	ures
5	0	12		0
2000	0	0		0
Vlan	Dest MAC Failures	s IP Valida	tion Failures	
5	(C	9	
2000	(C	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 ins	pection statis	stics vlan 5	
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
5	3	4618	4605	4
Vlan	DHCP Permits	ACL Permits	Source MAC Fail	lures
5	0	12		0
Vlan	Dest MAC Failur	es IP Valida	tion 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
       Configuration Operation
Vlan
                               ACL Match
                                               Static ACL
                               _____
                                               _____
 _ _ _ _
  5
                    Active second
       Enabled
                                               No
                    DHCP Logging
Vlan
       ACL Logging
 ____
       _____
                     _____
  5
       Acl-Match
                      A11
```

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) Displ	ay begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Displ	ay excludes lines that match the <i>expression</i> .
	include	(Optional) Displ	ay includes lines that match the specified <i>expression</i> .
	expression	Expression in th	e output to use as a reference point.
Command Modes	User EXEC		
Command History	Release	Modification	
	12.2(25)EX	This command w	/as introduced.
Examples	This is an example of	output from the show	v ip dhcp snooping command.
Examples	Switch> show ip dhc Switch DHCP snoopin DHCP snooping is co	p snooping g is enabled	
	40-42 Insertion of option Option 82 on untrus Verification of hwa	ted port is allowe	
	Interface	Trusted	Rate limit (pps)
	GigabitEthernet0/1 GigabitEthernet0/2	yes yes	unlimited unlimited
Related Commands	Command	Desc	ription
	ahow in dhan anooni	ng hinding Dian	ays the DHCP snooping binding information.
	show ip dhcp snoopi	ing binding Displ	ays the DHCF shooping 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	(Ontional)	pacify the hindi	ng entry IP addre	6.6			
Syntax Description	mac-address			ng entry MAC ad				
	interface interface-id			ng input interface				
	vlan vlan-id			ng entry VLAN.				
	begin	· • ·		that matches the	arprass	sion		
	exclude	1 1 1			·	aon.		
	include	1,1	Display excludes lines that match the <i>expression</i> .					
	expression	Expression	in the output to t	ise as a reference	point.			
Command Modes	User EXEC							
Command History	Release	Modification	n					
	12.2(25)EX	This comma	and was introduc	ed.				
Usage Guidelines	Use the show ip sour configured bindings i If DHCP snooping is	ce binding privil n the DHCP snow enabled and an in	leged EXEC con oping binding da	nmand to display tabase.	the dyr	lly configured bindings namically and statically witch does not delete the		
	statically configured bindings.							
	Expressions are case and do not appear, but the				ut, the l	lines that contain <i>outpu</i> .		
Examples	This example shows h	now to display th	e DHCP snoopir	ng binding entries	for a s	witch:		
	Switch> show ip dho MacAddress	IpAddress	Lease(sec)	Туре	VLAN	Interface		
	01:02:03:04:05:06 00:D0:B7:1B:35:DE Total number of bin	10.1.2.150	9837 237	dhcp-snooping dhcp-snooping	20 20 20	GigabitEthernet0/1 GigabitEthernet0/2		

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

Switch> show ip dho MacAddress	p snooping bindi IpAddress	.ng 10.1.2.150 Lease(sec)		VLAN	Interface
01:02:03:04:05:06 Total number of bir		9810	dhcp-snooping	20	GigabitEthernet0/1

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

Switch> show ip dhe	p snooping bindin	g 0102.0304.	0506		
MacAddress	IpAddress	Lease(sec)	Туре	VLAN	Interface
01:02:03:04:05:06	10.1.2.150	9788	dhcp-snooping	20	GigabitEthernet0/2
Total number of bin	dings: 1				

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

Switch> show ip dho	p snooping bindin	g interface	gigabitethernet	0/2	
MacAddress	IpAddress	Lease(sec)	Туре	VLAN	Interface
00:30:94:C2:EF:35	10.1.2.151	290	dhcp-snooping	20	GigabitEthernet0/2
Total number of bin	dings: 1				

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

Switch> show ip dho	p snooping bindin	ıg vlan 20			
MacAddress	IpAddress	Lease(sec)	Туре	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 bir	ndings: 2				

Table 2-11 describes the fields in the show ip dhcp snooping binding command output:

Table 2-11show 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	
Туре	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

S	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 <i>expression</i> .					
	exclude	I exclude(Optional) Display excludes lines that match the <i>expression</i> .I include(Optional) Display includes lines that match the specified <i>expression</i> . <i>expression</i> Expression in the output to use as a reference point.					
	include						
	expression						
Command Modes	User EXEC						
Command Modes	User EAEC						
Command History	Release	Modification					
	12.2(25)EX	This command was introduced.					
Examples	This is an exa	ample of output from the show ip dhcp snooping database command:					
	Agent URL : Write delay	v ip dhcp snooping database Timer : 300 seconds : 300 seconds					
	-	ng : No Expiry : Not Running Expiry : Not Running					
	Last Failed	ed Time : None Time : None Reason : No failure recorded.					
	Total Attemp	ots : 0 Startup Failures : 0					
	Successful 7						
	Successful H						
	Successful V Media Failur						
	This is an example of output from the show ip dhcp snooping database detail command:						
	Agent URL : Write delay	<pre>v ip dhcp snooping database detail tftp://10.1.1.1/directory/file Timer : 300 seconds : 300 seconds</pre>					
	-	ng : No Expiry : 7 (00:00:07) Expiry : Not Running					

Last Succeded Time :					
Last Failed Time : 17					
Last Failed Reason :	Unable t	o ac	cess 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 acce	ess: Read				
Last ignored bindings	counter	s :			
Binding Collisions	:	0	Expired leases	:	0
Invalid interfaces	:	0	Unsupported vlans	:	0
Parse failures	:	0			
Last Ignored Time : N	Ione				
Total ignored binding	gs counte	rs:			
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.

2-321

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 i	nformation.
	begin	(Optional) Display begins with the lin	e that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that	- -
	include	(Optional) Display includes lines that	
	expression	Expression in the output to use as a re	• •
Command Modes	User EXEC		
Command History	Release	Modification	
	12.2(37)SE	This command was introdu	ced.
Usage Guidelines	-	re case sensitive. For example, if you en	
Usage Guidelines	-	r, but the lines that contain <i>Output</i> appea	
Usage Guidelines	-		
Usage Guidelines Examples	do not appear		r.
	do not appear This is an exa Switch> show	, but the lines that contain <i>Output</i> appea ample of output from the show ip dhcp so y ip dhcp snooping statistics	r. snooping statistics command:
	do not appear This is an exa Switch> show Packets For	, but the lines that contain <i>Output</i> appear ample of output from the show ip dhcp s ip dhcp snooping statistics warded	r. snooping statistics command: = 0
	do not appear This is an exa Switch> show Packets For Packets Dro	, but the lines that contain <i>Output</i> appear ample of output from the show ip dhcp s ip dhcp snooping statistics warded	r. snooping statistics command:
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro	, but the lines that contain <i>Output</i> appea ample of output from the show ip dhcp s ip dhcp snooping statistics warded opped	r. snooping statistics command: = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa	, but the lines that contain <i>Output</i> appear ample of output from the show ip dhcp s ip dhcp snooping statistics warded apped popped From untrusted ports	r. snooping statistics command: = 0 = 0 = 0 = 0 snooping statistics detail command:
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro	but the lines that contain <i>Output</i> appear ample of output from the show ip dhcp so r ip dhcp snooping statistics warded apped poped From untrusted ports ample of output from the show ip dhcp so r ip dhcp snooping statistics detail pocessed by DHCP Snooping	r. snooping statistics command: = 0 = 0 = 0 = 0 snooping statistics detail command:
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro	where the lines that contain <i>Output</i> appears apple of output from the show ip dhcp so r ip dhcp snooping statistics warded apped apped From untrusted ports apple of output from the show ip dhcp so r ip dhcp snooping statistics detail bocessed by DHCP Snooping apped Because	r. snooping statistics command: = 0 = 0 = 0 = 0 snooping statistics detail command: = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro Dackets Dro IDB not k	where the lines that contain <i>Output</i> appears the provided of the second statistics the provided of the second statistics the provided of the second statistics the provided statistics of the second statistics of the secon	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro Dackets Dro LDB not k Queue ful	where the lines that contain <i>Output</i> appears the provided of the show in the	r. snooping statistics command: = 0 = 0 = 0 = 0 snooping statistics detail command: = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro IDB not k Queue ful Interface	where the lines that contain <i>Output</i> appears the provided of the second statistics the provided of the second statistics the provided of the second statistics the provided statistics of the second statistics of the secon	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro LDB not k Queue ful Interface Rate limi	the lines that contain <i>Output</i> appear ample of output from the show ip dhcp so ip dhcp snooping statistics warded apped apped From untrusted ports ample of output from the show ip dhcp so ip dhcp snooping statistics detail breessed by DHCP Snooping apped Because mown 1 is in errdisabled	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Pro Packets Dro IDB not k Queue ful Interface Rate limi Received Nonzero g	but the lines that contain <i>Output</i> appear ample of output from the show ip dhcp so ip dhcp snooping statistics warded apped apped From untrusted ports ample of output from the show ip dhcp so ip dhcp snooping statistics detail becessed by DHCP Snooping apped Because mown .1 is in errdisabled at exceeded on untrusted ports piaddr	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro IDB not k Queue ful Interface Rate limi Received Nonzero g Source ma	the lines that contain <i>Output</i> appear ample of output from the show ip dhcp so ip dhcp snooping statistics warded apped apped From untrusted ports ample of output from the show ip dhcp so ip dhcp snooping statistics detail accessed by DHCP Snooping apped Because mown 1 is in errdisabled t exceeded on untrusted ports giaddr ac not equal to chaddr	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro IDB not k Queue ful Interface Rate limi Received Nonzero g Source ma Binding m	the lines that contain <i>Output</i> appear ample of output from the show ip dhcp so ip dhcp snooping statistics warded apped apped From untrusted ports ample of output from the show ip dhcp so ip dhcp snooping statistics detail accessed by DHCP Snooping apped Because mown 1 a is in errdisabled at exceeded on untrusted ports giaddr ac not equal to chaddr hismatch	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro IDB not k Queue ful Interface Rate limi Received Nonzero g Source ma Binding m Insertior	the lines that contain <i>Output</i> appear ample of output from the show ip dhcp so ip dhcp snooping statistics warded apped apped From untrusted ports ample of output from the show ip dhcp so ip dhcp snooping statistics detail becessed by DHCP Snooping apped Because mown .1 a is in errdisabled at exceeded on untrusted ports giaddr at not equal to chaddr hismatch a of opt82 fail	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro IDB not k Queue ful Interface Rate limi Received Nonzero g Source ma Binding m Insertion	the lines that contain <i>Output</i> appear ample of output from the show ip dhcp so ip dhcp snooping statistics warded apped apped From untrusted ports ample of output from the show ip dhcp so ip dhcp snooping statistics detail becessed by DHCP Snooping apped Because mown .1 a is in errdisabled at exceeded on untrusted ports giaddr at not equal to chaddr hismatch a of opt82 fail a Down	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0
	do not appear This is an exa Switch> show Packets For Packets Dro Packets Dro This is an exa Switch> show Packets Pro Packets Dro DB not k Queue ful Interface Rate limi Received Nonzero g Source ma Binding m Insertion Interface Unknown of	the lines that contain <i>Output</i> appear ample of output from the show ip dhcp so ip dhcp snooping statistics warded apped apped From untrusted ports ample of output from the show ip dhcp so ip dhcp snooping statistics detail becessed by DHCP Snooping apped Because mown .1 a is in errdisabled at exceeded on untrusted ports giaddr at not equal to chaddr hismatch a of opt82 fail	r. snooping statistics command: = 0 = 0 = 0 snooping statistics detail command: = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0

Table 2-12 shows the DHCP snooping statistics and their descriptions:

Table 2-12	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.
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.

DHCP Snooping Statistic	Description
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 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.

Table 2-12 DHCP Snooping Statistics

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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	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.
Examples	_	es of output from the show ip igmp profile privileged EXEC command, with and g a profile number. If no profile number is entered, the display includes all profiles switch.
	Switch# show ip IGMP Profile 40 permit	
	Switch# show ip	igmp profile
	IGMP Profile 4 permit	9.0 230.9.9.0 9.0 229.255.255.255
Related Commands	range 230.9. IGMP Profile 4 permit	
Related Commands	range 230.9. IGMP Profile 4 permit range 229.9.	9.0 229.255.255.255

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 <i>expression</i> .	
	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 <i>output</i> appear.	
Examples	-	ble of output from the show ip igmp snooping vlan 1 command. It shows snooping or a specific VLAN.	
	Global IGMP Sno	p igmp snooping vlan 1 poping configuration:	
	IGMP snooping IGMPv3 snooping Report suppress TCN solicit que TCN flood query	ery :Disabled	

```
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
```

```
<u>Note</u>
```

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
                               :IGMP_ONLY
CGMP interoperability mode
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 <i>expression</i> .		
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .		
	include	(Optional) Display includes lines that match the specified <i>expression</i> .		
	expression	Expression in the output to use as a reference point.		
Command Modes	Privileged EXE	C		
Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
Usage Guidelines	Use this comma	and 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		
	-	case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> out the lines that contain <i>Output</i> 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	Туре	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 dy	namic
Vlan	Group	Туре	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	Туре	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

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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	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	VLAN IDs 1002 to snooping. When multicast VL	to display multicast router ports on the switch or for a specific VLAN. 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP AN registration (MVR) is enabled, the show ip igmp snooping mrouter command ticast router information and IGMP snooping information.
	-	e sensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> he lines that contain <i>Output</i> appear.
Examples	-	of output from the show ip igmp snooping mrouter command. It shows how to puter ports on the switch.
	Switch# show ip i Vlan ports	gmp snooping mrouter
	1 Gi0/1(dyn	amic)

Related

ed Commands	Command	Description
	ip igmp snooping	Enables and configures IGMP snooping on the switch or 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 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	n (Optional) Display begins with the line that matches the <i>expression</i> .				
	exclude	le (Optional) Display excludes lines that match the <i>expression</i> .				
	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	detected device multicast router	b igmp snooping querier command to display the IGMP version and IP address of a (also called a <i>querier</i>) that sends IGMP query message. A subnet can have multiple is but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast d as the querier. The querier can be a Layer 3 switch.				
	querier was dete	np snooping querier command output also shows the VLAN and interface on which the ected. If the querier is the switch, the output shows the <i>Port</i> field as <i>Router</i> . If the querier butput shows the port number on which the querier is learned in the <i>Port</i> field.				
	snooping queri	np snooping querier detail user EXEC command is similar to the show ip igmp er command. However, the show ip igmp snooping querier detail command displays of the most recent device detected by the switch querier along with this additional				
	• The elected	IGMP querier in the VLAN				
		uration and operational information pertaining to the switch querier (if any) that is in the VLAN				
		case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> out the lines that contain <i>Output</i> 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

	IP Address			Port
	1.1.1.1			Fa0/1
Global IG	MP switch queri	er statı	ıs	
max-respo querier-t tcn query tcn query Vlan 1:	sion address erval (sec) nse-time (sec) imeout (sec)	erier s	: 2 : 10 :atus	0
elected g	uerier is 1.1.1		on p	
admin sta admin ver source IP query-int max-respo querier-t tcn query tcn query operation operation	te sion address erval (sec) nse-time (sec) imeout (sec) count interval (sec)		: Enable : 2 : 10.1.1 : 60 : 10 : 120 : 2	ed 65

Related Commands

s 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]

	Switch> show ip sou MacAddress 	IpAddress 11.0.0.1 11.0.0.2	Lease(sec) infinite 10000 Description Configures the D Configures static	Type static dhcp-snooping HCP snooping bi	VLAN 10 10			
Examples Related Commands	Switch> show ip sou MacAddress 00:00:00:0A:00:0B 00:00:00:0A:00:0A	IpAddress 11.0.0.1 11.0.0.2	infinite 10000 Description	Type static dhcp-snooping	VLAN 10 10	GigabitEthernet0/1 GigabitEthernet0/1		
Examples	Switch> show ip sou MacAddress 00:00:00:0A:00:0B	IpAddress 11.0.0.1	infinite	Type static	VLAN 10	GigabitEthernet0/1		
Examples	Switch> show ip sou MacAddress	IpAddress		_		Interface		
Examples	1			omung comman	d:			
	This is an example of	output from th	e show ip source	hinding common				
Usage Guidelines	The show ip source b in the DHCP snoopin command to display c	g binding datab	base. Use the show	ip dhcp snoopii		ally configured binding ling privileged EXEC		
	12.2(50)SE	This comm	nand was introduce	ed.				
Command History	Release	Modificati	on					
Command Modes	User EXEC							
	expression	Expression i	in the output to use	e as a reference p	oint.			
	include		Display includes lin					
	exclude							
	interface interface-id(Optional) Display IP source bindings on a specific interface.I begin(Optional) Display begins with the line that matches the expression.							
	interface interface-id			• •				
	vlan vlan-id		Display static IP so Display IP source b		sific VI			
	dhcp-snooping static		1 1		e learne	ed by DHCP snooping.		
	mac-address							
	maa addrage) Display IP source bindings for a specific IP address.) Display IP source bindings for a specific MAC address.					

show ip verify source

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

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

Syntax Description	interface	interface <i>interface-id</i> (Optional) Display IP source guard configuration on a specific interface.					
	begin		(Optional) Di	splay begins with	h the line that matche	es the expression.	
	exclude	l exclude (Optional) Display excludes lines that match the <i>expression</i> .					
	include						
	expression	!			e as a reference point	•	
		·	2			·	
Command Modes	User EXEC	C					
Command History	Release		Modification				
	12.2(50)SI	F.		was introduced.			
		1 6 4		• • • • •			
Examples	This is an example of output from the show ip verify source command:						
		how ip verify Filter-type	source 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-tru	-			
	fa0/3	ip		snooping-vlan		1.0	
	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		
	fa0/4	ip-mac	active	deny-all	deny-all	12-20	
	fa0/5 fa0/5	ip-mac ip-mac	active active	10.0.0.3 deny-all	permit-all permit-all	10 11-20	
	In the prev	ious example,	this is the IP so	urce guard config	guration:		
	VLAN interfa default	s 10 to 20. For ce, and a bindi	VLAN 10, IP s ng is on the inte ontrol list (ACL)	source guard with erface. For VLAN	n IP address filtering Ns 11 to 20, the secor		
	• The Fa	• The Fast Ethernet 0/2 interface is configured as trusted for DHCP snooping.					
	enable	d, and static IF fault port ACL	source binding	s are configured	on VLANs 10 and 1	C address filtering is 1. For VLANs 12 to 20 P source guard is not	

• 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 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]

۵, Note

LACP is available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs).

	abannal aroun numbar	(Optional) Number of the channel group. The range is 1 to 48.				
Syntax Description	channel-group-number 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 <i>expression</i> .				
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .				
	include	(Optional) Display includes lines that match the specified <i>expression</i> .				
	<i>expression</i> Expression in the output to use as a reference point.					
Command Modes	User EXEC					
Command Modes	User EXEC	Modification				
		Modification This command was introduced.				
	Release 12.2(25)EX You can enter any show					
Command History	Release 12.2(25)EX You can enter any show specific channel informa	This command was introduced. lacp command to display the active channel-group information. To display				
Command History	Release 12.2(25)EX You can enter any show specific channel informa If you do not specify a change	This command was introduced. lacp command to display the active channel-group information. To display tion, enter the show lacp command with a channel-group number.				

Examples

This is an example of output from the **show lacp counters** user EXEC command. Table 2-13 describes the fields in the display.

Switch> show	w lacp o	counters					
	LAC	PDUs	Marl	ker	Marker H	Response	LACPDUs
Port	Sent	Recv	Sent	Recv	Sent	Recv	Pkts Err
Channel grou	.1:1						
Gi0/1	19	10	0	0	0	0	0
Gi0/2	14	6	0	0	0	0	0

Table 2-13show 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
                              Priority
                                            Key
                                                      Кеу
                                                                        State
                    State
                                                               Number
Gi0/1
                              32768
            SA
                    bndl
                                            0x3
                                                       0x3
                                                               0x4
                                                                        0x3D
Gi0/2
            SA
                    bndl
                              32768
                                            0x3
                                                       0x3
                                                               0x5
                                                                        0x3D
```

Table 2-14 describes the fields in the display.

Table 2-14show 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.				

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

 Table 2-14
 show lacp internal Field Descriptions (continued)

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

Flags: S	show lacp neighbor 5 - Device is sending A - Device is in Activ			-			
Channel group 3 neighbors							
Partner's	s information:						
Port Gi0/1	32768,0007.eb49.5e80 LACP Partner	Partner Port Number OxC Partner Oper Key Ox3	Age 19s Partner Port State 0x3C	Partner Flags SP			
Partner's	s information:						
Port Gi0/2	··· 1 ··· ··	Partner Port Number 0xD	Age 15s	Partner Flags SP			
	LACP Partner Port Priority 32768	Partner Oper Key 0x3	Partner Port State 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.

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.	
	clear lacp lacp port-priority	

show mac access-group

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

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

Syntax Description	interface interface-id	(Optional) Display the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port-channel range is 1 to 48 (available only in privileged EXEC mode).
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified 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	-	nsitive. For example, if you enter exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear.
Usage Guidelines Examples	do not appear, but the li This is an example of ou	nes that contain <i>Output</i> appear. utput from the show mac-access group user EXEC command. In this display, 0/2 has the MAC access list <i>macl_e1</i> applied to inbound traffic; no MAC ACLs

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) D	isplay begins with the line that matches the <i>expression</i> .
	exclude	(Optional) D	isplay excludes lines that match the <i>expression</i> .
	include	(Optional) D	isplay includes lines that match the specified expression.
	expression	Expression i	n the output to use as a reference point.
ommand Modes	User EXEC		
ommand History	Release	Modification	I
	12.2(25)EX	This comma	nd was introduced.
sage Guidelines	-	case sensitive. For exa at the lines that contain	mple, if you enter exclude output , the lines that contain <i>outp</i> in <i>Output</i> appear.
	do not appear, bu This is an examp Switch> show ma Mac 2	ut the lines that contain ole of output from the s ac address-table Address Table	n <i>Output</i> appear. show mac address-table command:
-	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add	ut the lines that contain the of output from the s ac address-table Address Table dress Type	show mac address-table command:
	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add	ut the lines that contain the of output from the s ac address-table Address Table dress Type	<i>Output</i> appear. show mac address-table command:
	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00	at the lines that contain the of output from the state ac address-table Address Table Address Type 	h Output appear. show mac address-table command: Ports CPU CPU CPU
	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00	at the lines that contain ble of output from the second stable Address Table Address Type 000.0001 STATIC 000.0002 STATIC 000.0003 STATIC	h Output appear. show mac address-table command: Ports CPU CPU CPU CPU
	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00 All 0000.00	at the lines that contain ble of output from the second stable Address Table Address Type Address Type Addres	h Output appear. show mac address-table command: Ports CPU CPU CPU CPU CPU CPU
	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00	at the lines that contain ble of output from the second stable address Table dress Type 	A Output appear. show mac address-table command: Ports CPU CPU CPU CPU CPU CPU CPU
	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0180.c2	at the lines that contain ble of output from the second stable address Table address Type address Type addres	A Output appear. show mac address-table command: Ports CPU CPU CPU CPU CPU CPU CPU CPU
-	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0180.c2 All 0180.c2	at the lines that contain a contrast from the second seco	A Output appear. show mac address-table command: Ports CPU CPU CPU CPU CPU CPU CPU CPU
-	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0180.c2 All 0180.c2 All 0180.c2	at the lines that contain a contrast from the second seco	A Output appear. show mac address-table command: Ports CPU CPU CPU CPU CPU CPU CPU CPU
lsage Guidelines xamples	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0180.c2 All 0180.c2 All 0180.c2 All 0180.c2	at the lines that contain a contrast from the second seco	A Output appear. show mac address-table command: Ports CPU CPU CPU CPU CPU CPU CPU CPU
	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0180.c2 All 0180.c2 All 0180.c2 All 0180.c2 All 0180.c2	at the lines that contain a contrast from the second seco	A Output appear. show mac address-table command: Ports CPU CPU CPU CPU CPU CPU CPU CPU
	do not appear, bu This is an examp Switch> show ma Mac A Vlan Mac Add All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0000.00 All 0180.c2 All 0180.c2 All 0180.c2 All 0180.c2 All 0180.c2 All 0180.c2 All 0180.c2	at the lines that contain a contrast from the second seco	A Output appear. show mac address-table command: Ports CPU CPU CPU CPU CPU CPU CPU CPU

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					
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 <i>expression</i> .			
	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			
Command History	Release 12.2(25)EX	Modification This command was introduced.			
	12.2(25)EX Expressions are case ser	This command was introduced.			
Usage Guidelines	12.2(25)EX Expressions are case ser do not appear, but the lin	This command was introduced.			
Command History Usage Guidelines Examples	12.2(25)EX Expressions are case ser do not appear, but the lin This is an example of ou	This command was introduced. Insitive. For example, if you enter exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear. Intput from the show mac address-table address command: ress-table address 0002.4b28.c482			
Usage Guidelines	12.2(25)EX Expressions are case ser do not appear, but the lin This is an example of ou Switch# show mac addr	This command was introduced. Insitive. For example, if you enter exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> appear. Intput from the show mac address-table address command: ress-table address 0002.4b28.c482			

Related Commands C

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 <i>expression</i> .
	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 v Ernv numbe	er is specified, the aging time for all VLANs appears.
	-	se sensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> he lines that contain <i>Output</i> appear.
Examples	do not appear, but t	se sensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> he lines that contain <i>Output</i> appear. of output from the show mac address-table aging-time command:
Examples	do not appear, but t This is an example Switch> show mac Vlan Aging Tim	he lines that contain <i>Output</i> appear. of output from the show mac address-table aging-time command: address-table aging-time ne
Examples	do not appear, but t This is an example Switch> show mac	he lines that contain <i>Output</i> appear. of output from the show mac address-table aging-time command: address-table aging-time ne
Examples	do not appear, but t This is an example Switch> show mac Vlan Aging Tim 1 300	he lines that contain <i>Output</i> appear. of output from the show mac address-table aging-time command: address-table aging-time ne
Examples	do not appear, but t This is an example Switch> show mac Vlan Aging Tim 1 300 This is an example	he lines that contain <i>Output</i> appear. of output from the show mac address-table aging-time command: address-table aging-time he of output from the show mac address-table aging-time vlan 10 command: address-table aging-time vlan 10 he

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 <i>expression</i> .
	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 nu	mber is specified, the address count for all VLANs appears.
eouge cultoniloo		e case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i>
	-	but the lines that contain <i>Output</i> appear.
Examples	This is an exam	ple of output from the show mac address-table count command:
·		nac address-table count
	Dynamic Addres Static Addres Total Mac Addr	as Count : 0
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 <i>interfaces</i> 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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	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		se sensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> the lines that contain <i>Output</i> appear.
Examples	Switch> show mac	of output from the show mac address-table dynamic command: address-table dynamic dress Table
	Vlan Mac Addr	
	1 00b0.649	5.7862 DYNAMIC Gi0/2 6.2741 DYNAMIC Gi0/2 ses 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 <i>expression</i> .	
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
	I include (Optional) Display includes lines that match the specified <i>expression</i> .		
	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	-	sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> e lines that contain <i>Output</i> appear.	
Examples	This is an example o	f output from the show mac address-table interface command:	
Examples	Switch> show mac a	f output from the show mac address-table interface command: ddress-table interface gigabitethernet0/2 ress Table	
Examples	Switch> show mac a Mac Addr Vlan Mac Addres	ddress-table interface gigabitethernet0/2 ess Table 	
Examples	Switch> show mac a Mac Addr Vlan Mac Addres	ddress-table interface gigabitethernet0/2 ess Table 	
Examples	Switch> show mac a Mac Addr Vlan Mac Addres 1 0030.b635. 1 00b0.6496.	ddress-table interface gigabitethernet0/2 ess Table s Type Ports 	

Related Commands Co

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

show mac address-table notification

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

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

Syntax Description	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 <i>expression</i> .	
	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.	
	Use the interface keyword to display the flags for all interfaces. If the <i>interface-id</i> is included, only the flags for that interface appear.		
	Expressions are case sensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.		
Examples	This is an example	e of output from the show mac address-table notification command:	
	<pre>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</pre>		
	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 : MAC Addr: 0000.0000.0000 Module: 0 Operation: Deleted Vlan: 2 Port: 1 Operation: Deleted Vlan: 2MAC Addr: 0000.0000.0001 Module: 0Operation: Deleted Vlan: 2MAC Addr: 0000.0000.0002 Module: 0 Port: 1 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 <i>interfaces</i> 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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	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 do not appear, but the lines that contain <i>Output</i> appear.	
Examples		of output from the show mac address-table static command: address-table static

	Mac Address T	able	
Vlan	Mac Address	Туре	Ports
A11	0100.0ccc.cccc	STATIC	CPU
A11	0180.c200.0000	STATIC	CPU
A11	0100.0ccc.cccd	STATIC	CPU
A11	0180.c200.0001	STATIC	CPU
A11	0180.c200.0004	STATIC	CPU
A11	0180.c200.0005	STATIC	CPU
4	0001.0002.0004	STATIC	Drop
6	0001.0002.0007	STATIC	Drop
Total	Mac Addresses for	this cr	iterion: 8

Related Commands Co

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]

· · ·	vlan-id	(0 1)				
=		(Optional)	Display a	addresses for a specific VLAN. The range is 1 to 4094.		
-	begin (Optional) Display begins with the line that matches the <i>expression</i> .					
	exclude (Optional) Display excludes lines that match the <i>expression</i> .					
-	 include (Optional) Display includes lines that match the specified <i>expression</i> .					
-	expression	Expression	in the ou	atput to use as a reference point.		
Command Modes	User EXEC					
Command History	Release		Modificat	tion		
	12.2(25)EX		This com	mand was introduced.		
Fxamples	This is an exa	ample of out	out from t	he show mac address-table vlan 1 command [.]		
•	Switch> show Ma	ample of outp w mac addres ac Address T	s-table able			
-	Switch> shov Ma Vlan Mac	w mac addres ac Address T 	a s-table Type	vlan 1 Ports		
-	Switch> shov Ma Mac 	w mac addres ac Address T	a s-table Cable Type	vlan 1		
-	Switch> shov Ma Vlan Mac 1 0100	w mac addres ac Address T Address	a s-table Cable Type	vlan 1 Ports 		
-	Switch> show Ma 1 0100 1 0180	w mac address ac Address T Address 	s-table able Type STATIC STATIC	vlan 1 Ports CPU		
-	Switch> show Ma Mac 1 0100 1 0180 1 0100 1 0180	w mac address ac Address T Address 	Type STATIC STATIC STATIC STATIC STATIC	vlan 1 Ports CPU CPU CPU CPU CPU CPU		
-	Switch> show Ma 1 0100 1 0180 1 0180 1 0180 1 0180	w mac address ac Address T Address 	Type STATIC STATIC STATIC STATIC STATIC STATIC STATIC	vlan 1 Ports CPU CPU CPU CPU CPU CPU CPU CPU		
-	Switch> show Ma 1 0100 1 0180 1 0180 1 0180 1 0180 1 0180	w mac address ac Address T Address 	Type Type STATIC STATIC STATIC STATIC STATIC STATIC STATIC STATIC	vlan 1 Ports CPU		
-	Switch> show Ma 1 0100 1 0180 1 0180 1 0180 1 0180 1 0180 1 0180	<pre>w mac address ac Address T Address</pre>	Type Type STATIC STATIC STATIC STATIC STATIC STATIC STATIC STATIC STATIC	vlan 1 Ports CPU		
-	Switch> show Ma 1 0100 1 0180 1 0180 1 0180 1 0180 1 0180 1 0180 1 0180	w mac address ac Address T Address 	Type Type STATIC STATIC STATIC STATIC STATIC STATIC STATIC STATIC	vlan 1 Ports CPU		

Related Commands Co

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]

(Optional) Display information about specified SPAN sessions.numberSpecify the number of the SPAN or RSPAN session. The range is 1 to 66.Display all SPAN sessions.Display only local SPAN sessions.StDisplay a range of SPAN sessions, where <i>list</i> is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.NoteThis keyword is available only in privileged EXEC mode.Display only remote SPAN sessions.(Optional) Display detailed information about the specified sessions.Display begins with the line that matches the <i>expression</i> .eDisplay excludes lines that match the <i>expression</i> .eDisplay includes lines that match the specified <i>expression</i> .onExpression in the output to use as a reference point.
Display all SPAN sessions. Display only local SPAN sessions. St Display a range of SPAN sessions, where <i>list</i> is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges. Note This keyword is available only in privileged EXEC mode. Display only remote SPAN sessions. (Optional) Display detailed information about the specified sessions. Display begins with the line that matches the <i>expression</i> . e Display includes lines that match the specified <i>expression</i> .
Display only local SPAN sessions. St Display a range of SPAN sessions, where <i>list</i> is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges. Note This keyword is available only in privileged EXEC mode. Display only remote SPAN sessions. (Optional) Display detailed information about the specified sessions. Display begins with the line that matches the <i>expression</i> . e Display includes lines that match the specified <i>expression</i> .
St Display a range of SPAN sessions, where <i>list</i> is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges. Note This keyword is available only in privileged EXEC mode. Display only remote SPAN sessions. (Optional) Display detailed information about the specified sessions. Display begins with the line that matches the <i>expression</i> . e Display includes lines that match the specified <i>expression</i> .
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.NoteThis keyword is available only in privileged EXEC mode.Display only remote SPAN sessions.Display only remote SPAN sessions.(Optional) Display detailed information about the specified sessions.Display begins with the line that matches the expression.eDisplay excludes lines that match the expression.eDisplay includes lines that match the specified expression.
Display only remote SPAN sessions. (Optional) Display detailed information about the specified sessions. Display begins with the line that matches the <i>expression</i> . e Display excludes lines that match the <i>expression</i> . e Display includes lines that match the specified <i>expression</i> .
(Optional) Display detailed information about the specified sessions. Display begins with the line that matches the <i>expression</i> . e Display excludes lines that match the <i>expression</i> . e Display includes lines that match the specified <i>expression</i> .
Display begins with the line that matches the expression.eDisplay excludes lines that match the expression.eDisplay includes lines that match the specified expression.
e Display excludes lines that match the <i>expression</i> . e Display includes lines that match the specified <i>expression</i> .
Display includes lines that match the specified <i>expression</i> .
pn Expression in the output to use as a reference point
EC
Modification
EX This command was introduced.

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
   TX Unly:
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
                 1-9
   Both:
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
_____
                 :Local Session
Туре
Source Ports
                 :
   rce 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
                 :
                 :Fa0/1
   Both
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 <i>expression</i> .					
	include	nclude (Optional) Display includes lines that match the specified <i>expression</i> .					
	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.					
Examples	This is an example of	of output from the show mvr command:					
Examples	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						
	MVR Current multic MVR Global query i	cast groups: 0 response time: 5 (tenths of sec)					

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 <i>expression</i> .(Optional) Display includes lines that match the specified <i>expression</i> .					
	include						
	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

DWICCIII	DIION INVI	Incollago			
Port	Туре	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 interf	ace fa0/10			
Port	Туре	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 interf	ace fa0/1			
Port	Туре	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 inte	erface	gigabitet	hernet0/1	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]

I begin (Optional) Display begins with the life that matches the expression. I exclude (Optional) Display excludes lines that match the expression. I 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 I2.2(25)EX This command was introduced. I2.2(25)EX This command was introduced. I2.2(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, source ports are members of all multicast groups. Expressions are case sensitive. For example, if you enter I 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 VLAN Membership 239.1.1.1 ACTIVE Fa0/1 1 Statue 239.1.1.1 ACTIVE Fa0/1 1 Statue 239.1.1.2 ACTIVE Fa0/2 2 Statue 239.1.1.2 ACTIVE<	Syntax Description	<i>ip-address</i> (Optional) The IP multicast address. If the address is entered, all receiver source ports that are members of the multicast group appear. If no address entered, all members of all Multicast VLAN Registration (MVR) groups listed. If a group has no members, the group is listed as Inactive.					
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(25)EX The scommand 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, source ports are members of all multicast groups. Expressions are case sensitive. For example, if you enter l 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 Members VLAN Membership MVR Group Status Members VLAN Membership MVR Group Status Members VLAN Membership The ACTIVE Fa0/1 1 Status 239,1.1.1 ACTIVE Fa0/2 2 Status 239,1.1.2 ACTIVE Fa0/2 2 Status 239,1.1.2 ACTIVE Fa0/2<		begin					
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, source ports are members of all multicast groups. Expressions are case sensitive. For example, if you enter I 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 Switch# show mvr members MVR Group Statue 239.1.1.1 ACTIVE ACTIVE Fa0/1 239.1.1.1 ACTIVE ACTIVE Fa0/2 239.1.1.2 ACTIVE ACTIVE Fa0/1 239.1.1.2 ACTIVE ACTIVE Fa0/2 239.1.1.2 ACTIVE ACTIVE Fa0/2 239.1.1.2 ACTIVE		-		· •	· •		
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, source ports are members of all multicast groups. Expressions are case sensitive. For example, if you enter I exclude output, the lines that contain output on or appear, but the lines that contain Output appear. Examples This is an example of output from the show mvr members command: Switch# show wvr members Switch# show wvr members WK Group Status 239.1.1.1 ACTIVE ACTIVE Fa0/1 239.1.1.1 ACTIVE ACTIVE Fa0/2 239.1.1.2 ACTIVE ACTIVE Fa0/2 239.1.1.2 ACTIVE ACTIVE Fa0/2 239.1.1.2 ACTIVE ACTIVE Fa0/2 239.1.1.2 ACTIVE		include		(Optiona	l) Displ	ay includes lines that match the specified <i>expression</i> .	
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, source ports are members of all multicast groups. Expressions are case sensitive. For example, if you enter I 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 Members VLAN Members/VLAN Membership 239.1.1.1 ACTIVE Fa0/1 1 Static 239.1.1.1 ACTIVE Fa0/2 2 Static 239.1.1.2 ACTIVE Fa0/2 2 Static 239.1.1.2 ACTIVE Fa0/2 2 Static		expression		Expressio	on in th	e output to use as a reference point.	
I2.2(25)EX This command was introduced. I2.2(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, source ports are members of all multicast groups. Expressions are case sensitive. For example, if you enter I 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 Members VLAN MVR Group Status Members VLAN 239.1.1.1 ACTIVE Fa0/1 1 239.1.1.1 ACTIVE Fa0/1 2 Statuc 239.1.1.2 ACTIVE Fa0/2 2 Statuc 239.1.1.2 ACTIVE Fa0/2 2 Statuc	Command Modes	Privileged E2	XEC				
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, 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 ACTIVE Fa0/1 1 Static 239.1.1.1 ACTIVE Fa0/2 2 Static 239.1.1.1 ACTIVE 239.1.1.2 ACTIVE Fa0/2 2 Static 239.1.1.2 ACTIVE Fa0/2 2	Command History	Release		Modifica	tion		
Usage Guidelines The show mvr members command applies to receiver and source ports. For MVR-compatible mode, 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 ACTIVE Fa0/1 239.1.1.1 ACTIVE Static 239.1.1.1 ACTIVE Fa0/2 Static 239.1.1.1 ACTIVE Fa0/1 Static 239.1.1.1 ACTIVE Fa0/2 Static 239.1.1.1 ACTIVE Fa0/2 Static 239.1.1.2 ACTIVE Fa0/2 Static 239.1.1.2		12.2(25)EX		This com	mand w	vas introduced.	
Source ports are members of all multicast groups. Expressions are case sensitive. For example, if you enter exclude output, the lines that contain output on the appear. Examples This is an example of output from the show mvr members command: Switch# show mvr members MVR Group Status MVR Group Status MVR Group Status MVR Fall 1 Suitch# show mvr members 239.1.1.1 ACTIVE Fall 1 Static 239.1.1.1 ACTIVE Fall Static 239.1.1.1 ACTIVE Fall Static 239.1.1.1 ACTIVE Fall Static 239.1.1.2 ACTIVE Fall Static 239.1.1.2 ACTIVE Fall Static 239.1.1.2		12.2(35)SE		The VLA	N and	Membership fields were added to the output display.	
Switch# show mvr membersMVR GroupStatusMembersVLANMembership239.1.1.1ACTIVEFa0/11Static239.1.1.1ACTIVEFa0/22Static239.1.1.1ACTIVEFa0/22Static239.1.1.1ACTIVEFa0/23000Static239.1.1.2ACTIVEFa0/11Static239.1.1.2ACTIVEFa0/22Static239.1.1.2ACTIVEFa0/22Static	osage duidennes	source ports Expressions	are member are case sen	s of all mu sitive. For	lticast g exampl	groups. e, if you enter exclude output , the lines that contain <i>outpu</i>	
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 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	Examples	This is an ex	ample of ou	tput from t	he show	w mvr members command:	
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 239.1.1.1 ACTIVE Fa0/2 3000 Static 239.1.1.2 ACTIVE Fa0/1 1 Static 239.1.1.2 ACTIVE Fa0/2 2 Static		MVR Group	Status	Members		-	
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							
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				Fa0/1	2000	Static	
239.1.1.2 ACTIVE Fa0/1 1 Static 239.1.1.2 ACTIVE Fa0/2 2 Static		239.1.1.1	ACTIVE				
239.1.1.2 ACTIVE Fa0/2 2 Static		239.1.1.1	ACTIVE	Fa0/2		Static	
<output truncated=""></output>		239.1.1.1 239.1.1.1	ACTIVE ACTIVE	Fa0/2 Fa0/2	3000	Static Static	
		239.1.1.1 239.1.1.1 239.1.1.2	ACTIVE ACTIVE ACTIVE	Fa0/2 Fa0/2 Fa0/1	3000 1	Static Static Static	
		239.1.1.1 239.1.1.1 239.1.1.2 239.1.1.2	ACTIVE ACTIVE ACTIVE ACTIVE	Fa0/2 Fa0/2 Fa0/1	3000 1	Static Static Static	

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]]

۵, Note

PAgP is available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs).

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 <i>expression</i> .				
	exclude	(Optional) Display excludes lines that match the expression.				
	include	(Optional) Display includes lines that match the specified <i>expression</i> .				
	expression	Expression in the output to use as a reference point.				
Command Modes	User EXEC					
Commond Illiotom	Deleges	Modification				
Command History	Release					
	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.					
	-	sitive. For example, if you enter exclude output , the lines that contain <i>output</i> nes that contain <i>Output</i> are appear.				
Examples	do not appear, but the lin	nes that contain <i>Output</i> are appear.				
Examples	do not appear, but the lin	the show pagp 1 counters command:				
Examples	do not appear, but the lin This is an example of ou Switch> show pagp 1 co Informati	nes that contain <i>Output</i> are appear. Atput from the show pagp 1 counters command: Dunters ion Flush				
Examples	do not appear, but the lin This is an example of ou Switch> show pagp 1 co Informati Port Sent Re	nes that contain <i>Output</i> are appear. Atput from the show pagp 1 counters command: Sounters				
Examples	do not appear, but the lin This is an example of ou Switch> show pagp 1 co Informati Port Sent Re	hes that contain <i>Output</i> are appear. Atput from the show pagp 1 counters command: Dunters ion Flush ecv Sent Recv				

Gi0/1

Gi0/2

switch-p2

switch-p2

9s SC 10001

10001

24s SC

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

Switch>	sho	w pagp	1 inter	nal					
Flags:	s -	Devic	e is sen	ding Slo	w hello.	C - Dev	ice is in	Consisten	state.
	Α -	Devic	e is in .	Auto mod	e.				
Timers:	Н –	Hello	timer i	s runnin	g.	Q - Qui	t timer is	running.	
	S -	Switc	hing tim	er is ru	nning.	I - Inte	erface tim	er is run	ning.
Channel	gro	up 1							
					Hello	Partner	PAgP	Learning	Group
Port		Flags	State	Timers	Interval	Count	Priority	Method	Ifindex
Gi0/1		SC	U6/S7	Н	30s	1	128	Any	16
Gi0/2		SC	U6/S7	Н	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.

0002.4b29.4600 Gi0/1

0002.4b29.4600 Gi0/2

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.

Syntax Description	brief	(Optional) Display the name of each macro.
	description [interface <i>interface-id</i>]	(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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	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)EX Expressions are case sen	
Jsage Guidelines	12.2(25)EX Expressions are case sen	This command was introduced. Isitive. For example, if you enter exclude output , the lines that contain <i>outpu</i>
Usage Guidelines Examples	12.2(25)EX Expressions are case sen do not appear, but the lir	This command was introduced. Isitive. For example, if you enter exclude output , the lines that contain <i>outpu</i>
Usage Guidelines	12.2(25)EX Expressions are case sen do not appear, but the lin This is a partial output e Switch# show parser ma Total number of macros	This command was introduced. Asitive. For example, if you enter exclude output , the lines that contain <i>output</i> hes that contain <i>Output</i> appear. Asxample from the show parser macro command: acro
Jsage Guidelines	12.2(25)EX Expressions are case sen do not appear, but the lir This is a partial output e Switch# show parser ma	This command was introduced. Asitive. For example, if you enter exclude output , the lines that contain <i>output</i> hes that contain <i>Output</i> appear. Example from the show parser macro command: acro s = 2 acro1

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	<i>aggregate-policer-</i> (Optional) The name of the aggregate policer. <i>name</i>					
	begin	(Optional) Disp	Display begins with the line that matches the <i>expression</i> .			
	exclude	(Optional) Disp	lay excludes lines that match the <i>expression</i> .			
	include	(Optional) Disp	lay includes lines that match the specified expression.			
	expression	Expression in th	e output to use as a reference point.			
Command Modes	User EXEC					
Command History	Release	Modificatio)n			
	12.2(25)EX	This comm	and was introduced.			
Examples	This is an example	of output from the	e show policer aggregate command:			
	=	Switch> show policer aggregate my-policer aggregate-policer: my-policer				
	conform-ac	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 (j configuration)	policy-map class	Applies an aggregate policer to multiple classes in the same policy map.			
	policer aggregate configuration)	(global	Creates an aggregate policer to police all traffic received on an interface.			

show policer cpu uni-eni

Use the **show policer cpu uni-eni** user EXEC command to display control-plane policer information for the user network interfaces (UNIs) and enhanced network interfaces (ENIs) on the switch, including frames dropped or the configured threshold rate for the control-plane security feature on the switch.

show policer cpu uni-eni {drop [interface interface-id]] | rate} [| {begin | exclude | include}
expression]

Syntax Description	drop	(Optional) Display control-plane frame-drop count for all interfaces or the specified interface.
	interface <i>interface-id</i>	Optional) Display the control-plane information for the specified physical interface.
	rate	(Optional) Display the configured threshold rate for CPU policers.
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the expression.
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	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.
	12.2(44)SE	The show policer cpu uni command was changed to the show policer cpu uni-eni command.

Usage Guidelines

This command displays policer information that applies to UNIs and ENIs on the switch. Rate-limiting and policers are the same on both port types, except on ENIs on which a Layer 2 control protocol (CDP, STP, LLDP, LACP, or PAgP) has been enabled.

The output also displays if CPU protection has been disabled.

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

The **show policer cpu uni-eni 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-eni drop command.

Switch# show policer cpu uni-eni drop

=======================================		============
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-eni drop interface** command:

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

Switch> show policer cpu uni-eni rate CPU UNI/ENI port police rate = 160000 bps

This is an example of the show command output when CPU protection is disabled.

Switch# **show policer cpu uni-eni rate** CPU Protection feature is not enabled

Related Commands	Command	Description
	policer cpu uni	Configures a CPU policer threshold rate for the switch or enables or disables CPU protection.
	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:			
		• <i>interface-id</i> —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 <i>expression</i> .			
	I include (Optional) Display includes lines that match the specified <i>expression</i> .				
	<i>expression</i> Expression in the output to use as a reference point.				
Command History	Release	Modification			
Commanu mistory	12.2(25)EX	This command was introduced.			
Usage Guidelines	Expressions are case sens	itive. For example, if you enter exclude output , the lines that contain <i>output</i> es that contain <i>Output</i> appear.			
Examples	Switch> show policy-may				
	Policy Map videowizard_policy2 class videowizard_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
         Prioritv
    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)
  Oueue 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:
```

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
```

Tail Packets Drop: 191028

Table 2-15 describes the fields in the **show policy-map interface** display. The fields in the table are grouped according to the relevant QoS feature.

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 Service 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.			
Command	Description			
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.			

 Table 2-15
 show policy-map interface Field Descriptions

Related Commands

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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	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 (Count)	CurrentAddr (Count)	SecurityViolat (Count)	ion Security Action
Gi0/1	1	0	0	Shutdown
	in System (excl imit in System (5		

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	Туре	Ports	Remaining Age (mins)
1	0006.0700.0800	SecureConfigured	Gi0/2	1
Total	Addresses in System	(excluding one mag	ner port	• 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

	Jecure Mac Aud			
Vlan	Mac Address	Туре	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

LAN	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 [eni | nni | uni] [| {begin | exclude | include} expression]

Syntax Description	eni	Enhanced networ	k interface.				
	nni	Network node int	erface.				
	uni User network interface.						
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .					
	exclude		y excludes lines that match the <i>expression</i> .				
	include		y includes lines that match the specified <i>expression</i> .				
	expression	Expression in the	output to use as a reference point.				
ommand Modes	Privileged EXEC						
ommand History	Release	Modification					
_	12.2(25)EX	This command	was introduced.				
	12.2(44)SE	The eni keyword was added.					
	-	• •	le, if you enter I exclude output , the lines that contain <i>outpu</i> <i>Dutput</i> appear.				
Examples	This is an example Switch# show por Port Name	-	pw port-type command with no keywords:				
	 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)				
	H - 0 /11	1	User Network Interface (uni)				
	Fa0/11	1	USEL NECWOIK INCELLACE (UNII)				
	Fa0/11 Fa0/12	1	User Network Interface (uni)				

1

User Network Interface (uni)

Fa0/13

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) template that allocates system resources.

Syntax Description	layer-2	(Optional) Display resource all	locations for the template that supports Layer 2		
	v	features and does not support i	1 11 2		
	begin	(Optional) Display begins with	the line that matches the <i>expression</i> .		
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .			
	include	(Optional) Display includes lin	nes that match the specified expression.		
	expression	Expression in the output to use	e as a reference point.		
Command Modes	Privileged EXEC				
Command History	Release	Modification			
	12.2(25)EX	This command was introduce	ed.		
Usage Guidelines		played represent an approximate maxi ght vary, depending on the actual num	mum number for each feature resource. The nber of other features configured.		
Usage Guidelines	actual number mi	ght vary, depending on the actual num	nber of other features configured. er exclude output , the lines that contain <i>output</i>		
-	actual number mi Expressions are c do not appear, but	ght vary, depending on the actual num ase sensitive. For example, if you ente t the lines that contain <i>Output</i> appear.	nber of other features configured. er exclude output , the lines that contain <i>output</i>		
Usage Guidelines Examples	actual number mi Expressions are ca do not appear, but This is an exampl Switch# show sdu The current tem The selected ten the switch to su	ght vary, depending on the actual num ase sensitive. For example, if you enter t the lines that contain <i>Output</i> appear. The of output from the show sdm prefe	nber of other features configured. er l exclude output , the lines that contain <i>output</i> er command, displaying the template in use:		

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), enhanced network interfaces (ENIs), VLANs, and NNI or ENI 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	(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode).		
[detail interface interface_id [detail]]	The keywords have these meanings:		
interface-id [detail]]	• 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 <i>txholdcount</i> field was added.		
	The new master role appears for boundary ports.		
	The word <i>pre-standard</i> or <i>Pre-STD</i> appears when an IEEE standard bridge sends prestandard BPDUs on a port.		
	The word <i>pre-standard</i> (<i>config</i>) or <i>Pre-STD-Cf</i> appears when a port has been configured to send prestandard BPDUs and no prestandard BPDU has been received on that port.		
	The word <i>pre-standard</i> (<i>rcvd</i>) or <i>Pre-STD-Rx</i> appears when a prestandard BPDU has been received on a port that has not been configured to send prestandard BPDUs.		
	A <i>dispute</i> flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated.		
	• <i>instance-id</i> —You can specify a single instance ID, a range of IDs separated by a hyphen, or a series of IDs separated by a comma. The range is 1 to 4094. The display shows the number of currently configured instances.		
	• interface <i>interface-id</i> —(Optional) Valid interfaces include VLANs, physical NNIs and NNI port channels, and physical ENIs and ENI 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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.
Command Modes	User EXEC	
Command History	Release N	lodification
	12.2(25)EX T	his command was introduced.
	12.2(25)SEG T	he digest keyword was added, and new digest and transmit hold count
	fi	elds appear.
Usage Guidelines	STP is not supported on UN	elds appear. IIs. Valid spanning-tree information is available only for NNIs or ENIs.
Usage Guidelines	STP is not supported on UN If the <i>vlan-id</i> variable is om	elds appear. IIs. Valid spanning-tree information is available only for NNIs or ENIs. itted, the command applies to the spanning-tree instance for all VLANs. ve. For example, if you enter exclude output , the lines that contain <i>outpu</i>
-	STP is not supported on UN If the <i>vlan-id</i> variable is om Expressions are case sensiti do not appear, but the lines	elds appear. IIs. Valid spanning-tree information is available only for NNIs or ENIs. itted, the command applies to the spanning-tree instance for all VLANs. ve. For example, if you enter exclude output , the lines that contain <i>outpu</i>
Usage Guidelines Examples	STP is not supported on UN If the <i>vlan-id</i> variable is om Expressions are case sensiti do not appear, but the lines This is an example of output Switch# show spanning-tr VLAN0001 Spanning tree enabled Root ID Priority Address Cost Port	elds appear. IIs. Valid spanning-tree information is available only for NNIs or ENIs. itted, the command applies to the spanning-tree instance for all VLANs. ve. For example, if you enter exclude output , the lines that contain <i>output</i> that contain <i>Output</i> appear. It from the show spanning-tree active command: ee active
-	STP is not supported on UN If the <i>vlan-id</i> variable is om Expressions are case sensiti do not appear, but the lines This is an example of output Switch# show spanning-tr VLAN0001 Spanning tree enabled : Root ID Priority Address Cost Port Hello Time Bridge ID Priority Address Hello Time Aging Time	elds appear. WIs. Valid spanning-tree information is available only for NNIs or ENIs. hitted, the command applies to the spanning-tree instance for all VLANs. ve. For example, if you enter exclude output, the lines that contain output that contain Output appear. It from the show spanning-tree active command: ee active protocol ieee 32768 0001.42e2.cdd0 3038 24 (GigabitEthernet0/1) 2 sec Max Age 20 sec Forward Delay 15 sec 49153 (priority 49152 sys-id-ext 1) 0003.fd63.9580 2 sec Max Age 20 sec Forward Delay 15 sec
	STP is not supported on UN If the <i>vlan-id</i> variable is om Expressions are case sensiti do not appear, but the lines This is an example of output Switch# show spanning-tr VLAN0001 Spanning tree enabled Root ID Priority Address Cost Port Hello Time Bridge ID Priority Address Hello Time	elds appear. WIs. Valid spanning-tree information is available only for NNIs or ENIs. hitted, the command applies to the spanning-tree instance for all VLANs. ve. For example, if you enter exclude output, the lines that contain <i>output</i> that contain <i>Output</i> appear. It from the show spanning-tree active command: ee active protocol ieee 32768 0001.42e2.cdd0 3038 24 (GigabitEthernet0/1) 2 sec Max Age 20 sec Forward Delay 15 sec 49153 (priority 49152 sys-id-ext 1) 0003.fd63.9580 2 sec Max Age 20 sec Forward Delay 15 sec

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>

output transation

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
                     is disabled by default
Portfast
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
Pathcost method used is short
                       Blocking Listening Learning Forwarding STP Active
Name

        1
        0
        0
        11

        3
        0
        0
        1

        3
        0
        0
        1

        3
        0
        0
        1

        3
        0
        0
        1

                                                                 12
VLAN0001
VLAN0002
                                                                    4
                         3
VLAN0004
                                                                   4
VLAN0006
                                                                   4
                                             0
VLAN0031
                          3
                                  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
```

This is 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 20000 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	e 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 Co

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]

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 <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.
	broadcast multicast unicast begin exclude include

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 td="" trun<=""><td>.cated></td><td></td><td></td><td></td></output>	.cated>			

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	gigabitether	net 0/1	
Interface	Filter State	Upper	Lower	Current
Gi0/1	Forwarding	20 pps	10 pps	5 pps

Table 2-16 describes the fields in the **show storm-control** display.

Table 2-16show 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 <i>expression</i> .			
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .			
	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.			
	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 quotern MTU	refere to parts operating at 10/100 Mbrs, the system jumbe MTU refers to Cigabit			
	ports. Expressions are ca	se sensitive. For example, if you enter exclude output , the lines that contain <i>output</i>			
Examples	ports. Expressions are ca do not appear, but	se sensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> the lines that contain <i>Output</i> appear.			

Sets the MTU size for the Fast Ethernet or Gigabit Ethernet ports.

system mtu

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.				
Evomploo		af autout from the shore table more assumed.				
Examples	This is an example	of output from the show table-map command:				
Examples	_	Le-map				
Examples	Switch> show tab tandoori_1>show t Table Map abc	Le-map Cable-map				
Examples	Switch> show tab tandoori_1>show t Table Map abc default copy Table Map cos2ds from 2 to 16	le-map cable-map				
Examples	Switch> show tabl tandoori_1>show tabl Table Map abc default copy Table Map cos2ds from 2 to 16 default copy Table Map cos2co from 2 to 5 from 3 to 6	le-map cable-map				

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 <i>expression</i> .				
	exclude	(Optional) Display excludes lines that match the expression.				
	l include (Optional) Display includes lines that match the specified <i>expression</i> .					
	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	the lines that contain <i>Output</i> appear. of output from the show udld <i>interface-id</i> command. For this display, UDLD is ids of the link, and UDLD detects that the link is bidirectional. Table 2-17 describes				
	the fields in this dis Switch> show udlo Interface gi0/1	splay. d gigabitethernet0/1				
	Port enable opera Current bidirecti Current operation Message interval Time out interval Entry 1 Expiration ti Device ID: 1 Current neigh Device name: Port ID: Gi0/ Neighbor echo	<pre>l: 5 ime: 146 hbor state: Bidirectional Switch-A /1 o 1 device: Switch-B o 1 port: Gi0/2</pre>				
	Message inter	rval: 5				

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).

Table 2-17 show udld Field Descriptions

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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	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	-	se sensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> the lines that contain <i>Output</i> appear.
Examples	Note Though vis	of output from the show version command: ible in the show version output, the <i>configuration register</i> information is not on the switch.
	(20050712:084347) Copyright (c) 198 Compiled Sun 17-J ROM: Bootstrap pr	re, MEAP Software (MEAP-IPSERVICES-M), Experimental Version 12.2 [teresang-meap-bug-fix 109] 36-2005 by Cisco Systems, Inc. Jul-05 13:19 by teresang rogram is C3750 boot loader
	tandoori_1 uptim System returned t System image file	Boot Loader (me3400-HBOOT-M), Version 12.2 [mbutts-meap2 103] ne is 1 day, 2 hours, 49 minutes to ROM by power-on e is "flash:image" 2-FA (PowerPC405) processor with 118784K/12280K bytes of memory.
	Processor board I Last reset from p Target IOS Versic 3 Virtual Etherne 24 FastEthernet i 2 Gigabit Etherne	power-on on 12.2(25)SE et interfaces .nterfaces

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

Swi	tch	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 | filter | id vlan-id | 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.
	filter	See the show vlan filter command.
	id vlan-id	(Optional) Display information about a single VLAN identified by VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094.
	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-enhanced network interface (UNI-ENI) VLAN information. Enter type (optional) to see only the VLAN ID and type of UNI-ENI 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** and **internal usage** keywords are 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) or enhanced network interfaced (ENIs) in a UNI-ENI community VLAN can communicate with each other; UNIs or ENIs in a UNI-ENI isolated VLAN cannot communicate. Network node interfaces (NNIs) can communicate with each other and with UNIs or ENIs in UNI-ENI 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 2-18 describes the fields in the display.



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.

VLAN	Name				Stat	tus Po	orts			
1	default			act:	Fa Fa Fa Fa	a0/5, H a0/9, H a0/13, a0/17,	Fa0/2, Fa(Fa0/6, Fa(Fa0/10, Fa Fa0/14, H Fa0/18, H Fa0/22, H Gi0/2)/7, Fa(a0/11, H Fa0/15, Fa0/19,)/8 Fa0/12 Fa0/16 Fa0/20	
L002	fddi-	default			act,	/unsup				
1003	token	-ring-defa	ault		act,	/unsup				
004	fddin	et-defaul	t		act,	/unsup				
1005 trnet-default			act,	/unsup						
/LAN	Туре	SAID	MTU	Parent	RingNo	BridgeNo	o Stp	BrdgMode	Trans1	Trans2
	enet	100001	1500	_	-	-	_	_	0	0
002	fddi	101002	1500	-	-	-	-	-	0	0
003	tr	101003	1500	-	-	-	-	-	0	0
004	fdnet	101004	1500	-	-	-	ieee	-	0	0
005	trnet	101005	1500 -	-	-	ibm -	0	0VLAN	Name	

Primary Seconda	ary Type	Ports	
VLAN Type	Ports		

Table 2-18show 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.	
Туре	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-ENI VLANs, the type (community or isolated), and the ports that belong to it.		

This is an example of output from the show vlan private-vlan command:

	show vlan Secondary	private-vlan 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 2	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
   UNI community
20
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
_____ _____
2 VLAN0200
                     active Gi0/1, Gi0/2
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
____ _____ ______
2
  enet 100002
            1500 -
                                    0
                                         0
                    _
Remote SPAN VLAN
_____
Disabled
```

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	-	sensitive. For example, if you enter l exclude output , the lines that contain <i>output</i> e lines that contain <i>Output</i> appear.
	do not appear, but th	e lines that contain <i>Output</i> appear.
Usage Guidelines Examples	do not appear, but th This is an example o Switch# show vlan Vlan access-map "S Match clauses:	e lines that contain <i>Output</i> appear. f output from the show vlan access-map command: access-map
	do not appear, but th This is an example o Switch# show vlan Vlan access-map "S Match clauses: ip address: S Action:	e lines that contain Output appear. f output from the show vlan access-map command: access-map ecWiz" 10 ecWiz_Fa1_0_3_in_ip Description
Examples	do not appear, but th This is an example o Switch# show vlan Vlan access-map "S Match clauses: ip address: S Action: forward	e lines that contain <i>Output</i> appear. f output from the show vlan access-map command: access-map wecWiz" 10 wecWiz_Fa1_0_3_in_ip
Examples	do not appear, but th This is an example of Switch# show vlan Vlan access-map "S Match clauses: ip address: S Action: forward Command	e lines that contain Output appear. f output from the show vlan access-map command: access-map lecWiz" 10 lecWiz_Fa1_0_3_in_ip Description Displays information about all VLAN filters or about a particular VLAN or

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.
	1 1 1 1	(optional) Display intering information for the specified v Livit 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 <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	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	1	ensitive. For example, if you enter exclude output , the lines that contain <i>output</i> lines that contain <i>Output</i> appear.
Examples	This is an example of	output from the show vlan filter command:
Examples	This is an example of Switch# show vlan f VLAN Map map_1 is f 20-22	ilter
Examples Related Commands	Switch# show vlan f VLAN Map map_1 is f	ilter
	Switch# show vlan f . VLAN Map map_1 is f. 20-22	ilter iltering VLANs: Description
	Switch# show vlan f: VLAN Map map_1 is f: 20-22	ilter iltering VLANs: Description Displays information about a particular VLAN access map or for all

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	
	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.
	do not appear, but the	e lines that contain <i>Output</i> appear.
Fromulae		
Examples		f output from the show vmps statistics command.
Examples	This is an example of Switch> show vmps a	f output from the show vmps statistics command.
Examples	This is an example of Switch> show vmps a VMPS Client Statist VQP Queries: VQP Responses:	f output from the show vmps statistics command. statistics 0 0
Examples	This is an example of Switch> show vmps a VMPS Client Statist VQP Queries: VQP Responses: VMPS Changes:	f output from the show vmps statistics command. statistics tics 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Examples	This is an example of Switch> show vmps a VMPS Client Statist VQP Queries: VQP Responses: VMPS Changes: VQP Shutdowns:	f output from the show vmps statistics command. statistics tics 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Examples	This is an example of Switch> show vmps a VMPS Client Statist VQP Queries: VQP Responses: VMPS Changes: VQP Shutdowns: VQP Denied:	f output from the show vmps statistics command. statistics tics 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Examples	This is an example of Switch> show vmps a VMPS Client Statist VQP Queries: VQP Responses: VMPS Changes: VQP Shutdowns:	f output from the show vmps statistics command. statistics 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Examples	This is an example of Switch> show vmps a VMPS Client Statist 	f output from the show vmps statistics command. statistics 0 0 0 0 0 0 0 0 0 0 0 0 0
Examples	This is an example of Switch> show vmps a VMPS Client Statist 	f output from the show vmps statistics command. statistics 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Table 2-19 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.

Field	Description
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 VersionNumber of times the version field in the query packet contains a value that is higher than th supported by the VMPS. The VLAN assignment of the port is not changed. The switches s VMPS Version 1 requests.	
VQP InsufficientNumber of times the VMPS is unable to answer the request because of a resource availabilitResourceIf the retry limit has not yet been reached, the client repeats the request with the same ser the next alternate server, depending on whether the per-server retry count has been reached	

Table 2-19 show vmps statistics Field Descriptions (continued)

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.