



Cisco ME 2400 Ethernet Access Switch Cisco IOS Commands

aaa accounting dot1x

Use the **aaa accounting dot1x** global configuration command to enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions. Use the **no** form of this command to disable IEEE 802.1x accounting.

no aaa accounting dot1x {*name |* **default**}

Syntax Description	name	Name of a server group. This is optional when you enter it after the broadcast group and group keywords.
	default	Use the accounting methods that follow as the default list for accounting services.
	start-stop	Send a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
	broadcast	Enable accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
	group	Specify the server group to be used for accounting services. These are valid server group names:
		• <i>name</i> —Name of a server group.
		• radius—List of all RADIUS hosts.
		• tacacs +—List of all TACACS+ hosts.
		The group keyword is optional when you enter it after the broadcast group and group keywords. You can enter more than optional group keyword.

aaa accounting dot1x {name | default} start-stop {broadcast group {name | radius | tacacs+}
 [group {name | radius | tacacs+} ...] | group {name | radius | tacacs+} [group {name | radius
 | tacacs+} ...]}

	radius	(Optional) Enable RADIUS authorization.	
	tacacs+	(Optional) Enable TACACS+ accounting.	
Defaults	AAA accounting is disabled.		
Command Modes	Global configuration		
Command History	Release Mo	dification	
2	12.2(25)EX Thi	s command was introduced.	
Usage Guidelines <u>×</u> Note	<u> </u>		
Examples	Switch(config)# aaa ac	to configure IEEE 802.1x accounting: counting dot1x counting dot1x default start-stop group radius	
Note	The RADIUS authentication server must be properly configured to accept and log update or watchdog packets from the AAA client.		
Related Commands	Command	Description	
	aaa authentication	Specifies one or more AAA methods for use on interfaces running	
	dot1x	IEEE 802.1x.	
	dot1x aaa-new-model		

dot1x timeout reauth	Sets the number of seconds between re-authentication attempts.
period	

aaa authentication dot1x

Use the **aaa authentication dot1x** global configuration command to specify the authentication, authorization, and accounting (AAA) method to use on ports complying with IEEE 802.1x. Use the **no** form of this command to disable authentication.

aaa authentication dot1x {default} method1

no aaa authentication dot1x {default}

tax Description	default	Use the listed authentication method that follows this argument as the default method when a user logs in.
	method1	Enter the group radius keywords to use the list of all RADIUS servers for
	memoar	authentication.
Note	Though other key keywords are supp	words are visible in the command-line help strings, only the default and group radius ported.
aults	No authentication	is performed.
mand Modes	Global configurat	ion
mand History	Release	Modification
	12.2(25)EX	This command was introduced.
ge Guidelines	The <i>method</i> argument identifies the method that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly IEEE 802.1x-compliant is the group radius method, in which the client data is validated against a RADIUS authentication server.	
	If you specify gro global configurati	up radius , you must configure the RADIUS server by entering the radius-server host on command.
	0 0	

Examples This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius

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

Related Commands	Command	Description
	aaa new-model	Enables the AAA access control model. For syntax information, see the Cisco IOS Security Command Reference, Release 12.2 > Authentication, Authorization, and Accounting > Authentication Commands.
	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.

action

Use the **action** access-map configuration command to set the action for the VLAN access map entry. Use the **no** form of this command to set the action to the default value, which is to forward.

action {drop | forward}

no action

Syntax Description	drop	Drop the packet when the specified conditions are matched.
	forward	Forward the packet when the specified conditions are matched.
Defaults	The default acti	on is to forward packets.
Command Modes	Access-map con	nfiguration
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	You enter access-map configuration mode by using the vlan access-map global configuration command. If the action is drop , you should define the access map, including configuring any access control list (ACL) names in match clauses, before applying the map to a VLAN, or all packets could be dropped.	
	In access-map of	configuration mode, use the match access-map configuration command to define the as for a VLAN map. Use the action command to set the action that occurs when a packet
	The drop and fo	prward parameters are not used in the no form of the command.
Examples	-	nows how to identify and apply a VLAN access map <i>vmap4</i> to VLANs 5 and 6 that causes orward an IP packet if the packet matches the conditions defined in access list <i>al2</i> :
	Switch(config- Switch(config- Switch(config-	<pre># vlan access-map vmap4 access-map)# match ip address al2 access-map)# action forward access-map)# exit # vlan filter vmap4 vlan-list 5-6</pre>
	You can verify	your settings by entering the show vlan access-map privileged EXEC command.

Related Commands	Command	Description
	access-list {deny permit}	Configures a standard numbered ACL. 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	Creates a named access list. 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	Creates a named MAC address access list.
	match (access-map configuration)	Defines the match conditions for a VLAN map.
	show vlan access-map	Displays the VLAN access maps created on the switch.
	vlan access-map	Creates a VLAN access map.

archive download-sw

Use the **archive download-sw** privileged EXEC command to download a new image from a TFTP server to the switch and to overwrite or keep the existing image.

archive download-sw {/force-reload | /imageonly | /leave-old-sw | /no-set-boot | /no-version-check | /overwrite | /reload | /safe} source-url

Syntax Description	/force-reload	Unconditionally force a system reload after successfully downloading the software image.
	/imageonly	Download only the software image but not the HTML files associated with the embedded device manager. The HTML files for the existing version are deleted only if the existing version is being overwritten or removed.
	/leave-old-sw	Keep the old software version after a successful download.
	/no-set-boot	Do not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded.
	/no-version-check	Download the software image without checking to prevent installing an incompatible image.
	/overwrite	Overwrite the software image in flash memory with the downloaded one.
	/reload	Reload the system after successfully downloading the image unless the configuration has been changed and not been saved.
	/safe	Keep the current software image; do not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download.
	source-url	The source URL alias for a local or network file system. These options are supported:
		• The syntax for the local flash file system: flash:
		 The syntax for the FTP: ftp:[[//username[:password]@location]/directory]/image-name.tar
		 The syntax for an HTTP server: http://[[username:password]@]{hostname / host-ip}[/directory]/image-name.tar
		 The syntax for a secure HTTP server: https://[[username:password]@]{hostname / host-ip}[/directory]/image-name.tar
		 The syntax for the Remote Copy Protocol (RCP): rcp:[[//username@location]/directory]/image-name.tar
		 The syntax for the TFTP: tftp:[[//location]/directory]/image-name.tar
		The <i>image-name</i> .tar is the software image to download and install on the switch.

Defaults	The current software image is not overwritten with the downloaded image.			
	Both the software image and HTML files are downloaded. The new image is downloaded to the flash: file system.			
	The BOOT environment variable is changed to point to the new software image on the flash: file system.			
	Image names are case sensitive; the image file is provided in tar format.			
	Compatibility of the version on the image to be downloaded is checked.			
Command Modes	Privileged EXEC			
Command History	Release Modification			
-	12.2(25)EXThis command was introduced.			
Usage Guidelines	The /imageonly option removes the HTML files for the existing image if the existing image is being removed or replaced. Only the Cisco IOS image (without the HTML files) is downloaded.			
	Using the /safe or /leave-old-sw option can cause the new image download to fail if there is insufficient flash memory. If leaving the software in place prevents the new image from fitting in flash memory due to space constraints, an error results.			
	If you used the /leave-old-sw option and did not overwrite the old image when you downloaded the new one, you can remove the old image by using the delete privileged EXEC command. For more information, see the "delete" section on page 2-52.			
Note	Use the /no-version-check option with care. This option allows an image to be downloaded without first confirming that it is not incompatible with the switch.			
	Use the /overwrite option to overwrite the image on the flash device with the downloaded one.			
	If you specify the command <i>without</i> the /overwrite option, the download algorithm verifies that the new image is not the same as the one on the switch flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded.			
	After downloading a new image, enter the reload privileged EXEC command to begin using the new image, or specify the / reload or / force-reload option in the archive download-sw command.			
Examples	This example shows how to download a new image from a TFTP server at 172.20.129.10 and overwrite the image on the switch:			
	Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar			
	This example shows how to download only the software image from a TFTP server at 172.20.129.10 to the switch:			
	Switch# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar			
	This example shows how to keep the old software version after a successful download:			
	Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar			

Related Commands	Command	Description
	archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.
	archive upload-sw	Uploads an existing image on the switch to a server.
	delete	Deletes a file or directory on the flash memory device.

archive tar

Use the **archive tar** privileged EXEC command to create a tar file, list files in a tar file, or extract the files from a tar file.

archive tar {/create destination-url flash:/file-url} | {/table source-url} | {/xtract source-url flash:/file-url [dir/file...]}

Syntax Description	/ create <i>destination-url</i> flash: /file-url	Create a new tar file on the local or network file system.
		For <i>destination-url, specify the</i> destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:
		• The syntax for the local flash filesystem: flash:
		 The syntax for the FTP: ftp:[[//username[:password]@location]/directory]/tar-filename.tar
		 The syntax for the Remote Copy Protocol (RCP) is: rcp:[[//username@location]/directory]/tar-filename.tar
		 The syntax for the TFTP: tftp:[[//location]/directory]/tar-filename.tar
		The <i>tar-filename</i> .tar is the tar file to be created.
		For flash: <i>/file-url, specify t</i> he location on the local flash file system from which the new tar file is created.
		An optional list of files or directories within the source directory can be specified to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.
	/table source-url	Display the contents of an existing tar file to the screen.
		For <i>source-url</i> , specify the source URL alias for the local or network file system. These options are supported:
		• The syntax for the local flash file system: flash:
		 The syntax for the FTP: ftp:[[//username[:password]@location]/directory]/tar-filename.tar
		 The syntax for the RCP: rcp:[[//username@location]/directory]/tar-filename.tar
		 The syntax for the TFTP: tftp:[[//location]/directory]/tar-filename.tar
		The <i>tar-filename.tar</i> is the tar file to display.

	/xtract source-url	Extract files from a tar file to the local file system.		
	flash: /file-url [dir/file]	For <i>source-url</i> , specify <i>the</i> source URL alias for the local file system. These options are supported:		
		• The syntax for the local flash file system: flash:		
		 The syntax for the FTP: ftp:[[//username[:password]@location]/directory]/tar-filename.tar 		
		 The syntax for the RCP: rcp:[[//username@location]/directory]/tar-filename.tar 		
		 The syntax for the TFTP: tftp:[[//location]/directory]/tar-filename.tar 		
		The <i>tar-filename</i> .tar is the tar file from which to extract.		
		For flash: / <i>file-url</i> [<i>dir/file</i>], specify <i>t</i> he location on the local flash file system into which the tar file is extracted. Use the <i>dir/file</i> option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted.		
Defaults	None			
Command Modes	Privileged EXEC			
Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
Usage Guidelines	Filenames and directory na	ames are case sensitive.		
	Image names are case sens	itive.		
Examples	This example shows how to create a tar file. The command writes the contents of the <i>new-configs</i> directory on the local flash device to a file named <i>saved.tar</i> on the TFTP server at 172.20.10.30:			
	Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs			
	This example shows how to display the contents of the file that is in flash memory. The contents of the tar file appear on the screen:			
	Switch# archive tar /table flash:me240x-metrobase-mz.122-25.EX.tar info (219 bytes) me240x-metrobase-mz.122-25.EX/(directory) me240x-metrobase-mz.122-25.EX (610856 bytes) me240x-metrobase-mz.122-25.EX/info (219 bytes) info.ver (219 bytes)			

This example shows how to display only the *html* directory and its contents:

```
Switch# archive tar /table flash:me240x-metrobase-mz.122-25.EX.tar me240x-metrobase-mz.12
-25/html
me240x-metrobase-mz.122-25.EX/html/ (directory)
me240x-metrobase-mz.122-25.EX/html/const.htm (556 bytes)
me240x-metrobase-mz.122-25.EX/html/xhome.htm (9373 bytes)
me240x-metrobase-mz.122-25.EX/html/menu.css (1654 bytes)
<output truncated>
```

This example shows how to extract the contents of a tar file on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local flash file system. The remaining files in the *saved.tar* file are ignored.

```
Switch# archive tar /xtract tftp:/172.20.10.30/saved.tar flash:/ new-configs
```

Related Commands	Command	Description
	archive download-sw	Downloads a new image from a TFTP server to the switch.
	archive upload-sw	Uploads an existing image on the switch to a server.

archive upload-sw

Use the **archive upload-sw** privileged EXEC command to upload an existing switch image to a server.

archive upload-sw [/version version_string] destination-url

Syntax Description	/version version_string	(Optional) Specify the specific version string of the image to be uploaded.	
	destination-url	The destination URL alias for a local or network file system. These options are supported:	
		• The syntax for the local flash file system: flash:	
		 The syntax for the FTP: ftp:[[//username[:password]@location]/directory]/image-name.tar 	
		 The syntax for the Remote Copy Protocol (RCP): rcp:[[//username@location]/directory]/image-name.tar 	
		 The syntax for the TFTP: tftp:[[//location]/directory]/image-name.tar 	
		The <i>image-name</i> .tar is the name of software image to be stored on the server.	
Command Modes	Privileged EXEC		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	Use the upload feature only if the HTML files associated with the embedded device manager have been installed with the existing image.		
	The files are uploaded in this sequence: the Cisco IOS image, the HTML files, and info. After these files are uploaded, the software creates the tar file.		
	Image names are case ser	nsitive.	
Examples	This example shows how	to upload the currently running image to a TFTP server at 172.20.140.2:	
	Switch# archive upload	l-sw tftp://172.20.140.2/test-image.tar	

Related Commands	Command	Description
	archive download-sw	Downloads a new image to the switch.
	archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.

bandwidth

Use the **bandwidth** policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ) by setting the output bandwidth for a policy-map class. Use the **no** form of this command to remove the bandwidth setting for the class.

bandwidth {*rate* | **percent** *value* | **remaining percent** *value*}

no bandwidth [*rate* | **percent** *value* | **remaining percent** *value*]

Syntax Description	rate	Set the bandwidth rate for the class in kilobits per second (kbps). The range is from 64 to 1000000.	
	percent value	Set the bandwidth for the class as a percent of the total bandwidth. The range is from 1 to 100 percent.	
	remaining percent	<i>value</i> Set the bandwidth for the class as a percent of the remaining bandwidth. The range is from 1 to 100 percent.	
Defaults	No bandwidth is def	ined.	
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 configure the bandwidth command in the class-default of an output policy map.	
Usage Guidelines	specifies the bandwi class from the bandw	dth policy-map class command to control output traffic. The bandwidth command dth for traffic in that class. CBWFQ derives the weight for packets belonging to the vidth allocated to the class and uses the weight to ensure that the queue for that class andwidth settings are not supported in input policy maps.	
	When you configure bandwidth for a class of traffic as an absolute rate (kbps) or a percentage of bandwidth (percent <i>value</i>), it represents the minimum bandwidth guarantee or committed information rate (CIR) for that traffic class. This means that the traffic class gets at least the bandwidth specified in the command, but is not limited to that bandwidth. Any excess bandwidth on the port is allocated to each class in the same ratio as the configured CIR rates.		
	only relative bandw	bandwidth remaining percent command, hard bandwidths are not guaranteed, and idths are assured. Class bandwidths are always proportional to the specified ges configured for the port.	
	When you configure bandwidth in an output policy, you must specify the same units in each bandwidth configuration; that is, all absolute values (rates) or percentages.		

The total rate of the minimum bandwidth guarantees for each queue of the policy cannot exceed the total speed for the interface. If the **percent** keyword is used, the sum of the class bandwidth percentages cannot exceed 100 percent.

Using the **queue-limit** command to modify the default queue limit is especially important on higher-speed interfaces so that they meet the minimum bandwidth guarantees required by the interface.

You cannot use the **bandwidth** policy-map class configuration command to configure CBWFQ and the **shape average** command to configure class-based shaping for the same class in a policy map.

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

Examples

This example shows how to set the precedence of output queues by setting bandwidth in kilobits per second. The classes *outclass1*, *outclass2*, and *outclass3* get a minimum of 50000, 20000, and 10000 kbps. The class **class-default** at a minimum gets the remaining bandwidth.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 50000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth 10000
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 output out-policy
Switch(config-if)# exit
```

This example shows how to set the precedence of output queues by allocating percentages of the total available bandwidth to each traffic class. The classes *outclass1*, *outclass2*, and *outclass3* get a minimum of 50, 20, and 10 percent. The class **class-default** at a minimum gets 20 percent.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# bandwidth percent 10
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 output out-policy
Switch(config-if)# exit
```

This example shows how to set *outclass1* as a priority queue, with *outclass2*, and *outclass3* getting 50 and 20 percent, respectively, of the bandwidth remaining after the priority queue is serviced. The class **class-default** gets the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# exit
Switch(config-j# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

You can verify your settings by entering the show policy-map privileged EXEC command.

Related Commands	Command	Description
	class	Defines a traffic classification match criteria for the specified class-map name.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	show policy-map	Displays quality of service (QoS) policy maps.

boot boothlpr

Use the **boot boothlpr** global configuration command to load a special Cisco IOS image, which when loaded into memory, can load a second Cisco IOS image into memory and launch it. This variable is used only for internal development and testing. Use the **no** form of this command to return to the default setting.

boot boothlpr *filesystem:/file-url*

no boot boothlpr

Syntax Description	filesystem:	Alias for a flash file system. Use flash: for the system board flash device.
	lfile-url	The path (directory) and name of a bootable helper image.
Defaults	No helper image is load	ded.
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
	Eilanomos and director	
Usage Guidelines	Filenames and directory names are case sensitive.	
		the setting of the BOOTHLPR environment variable. For more information, see E 2400 Ethernet Access Switch Boot Loader Commands"
Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot config-file

Use the **boot config-file** global configuration command to specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. Use the **no** form of this command to return to the default setting.

boot config-file flash:/*file-url*

no boot config-file

Syntax Description	flash: /file-url	The path (directory) and name of the configuration file.
Defaults	The default configu	ration file is flash:config.text.
Command Modes	Global configuration	n
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	Filenames and direc	ctory names are case sensitive.
	This command changes the setting of the CONFIG_FILE environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."	
Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot enable-break

Use the **boot enable-break** global configuration command to enable interrupting the automatic boot process. Use the **no** form of this command to return to the default setting.

boot enable-break

no boot enable-break

- **Defaults** Disabled. The automatic boot process cannot be interrupted by pressing the Break key on the console.
- Command Modes Global configuration

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

Usage Guidelines When you enter this command, you can interrupt the automatic boot process by pressing the break key on the console after the flash file system is initialized. The break key is different for each operating system:

- On a SUN work station running UNIX, Ctrl-C is the break key.
- On a PC running Windows 2000, Ctrl-Break is the break key.

This command changes the setting of the ENABLE_BREAK environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot helper

Use the **boot helper** global configuration command to dynamically load files during boot loader initialization to extend or patch the functionality of the boot loader. Use the **no** form of this command to return to the default.

boot helper *filesystem:/file-url* ...

no boot helper

Syntax Description	filesystem:	Alias for a flash file system. Use flash: for the system board flash device.	
	lfile-url	The path (directory) and a list of loadable files to dynamically load during loader initialization. Separate each image name with a semicolon.	
Defaults	No helper files are l	oaded.	
Command Modes	Global configuratio	n	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	This variable is used	d only for internal development and testing.	
	Filenames and directory names are case sensitive.		
		ages the setting of the HELPER environment variable. For more information, see ME 2400 Ethernet Access Switch Boot Loader Commands."	
Related Commands	Command	Description	

boot helper-config-file

Use the **boot helper-config-file** global configuration command to specify the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded. Use the **no** form of this command to return to the default setting.

boot helper-config-file filesystem:/file-url

no boot helper-config file

Syntax Description	filesystem:	Alias for a flash file system. Use flash: for the system board flash device.	
	lfile-url	The path (directory) and helper configuration file to load.	
Defaults	No helper configur	ation file is specified.	
Command Modes	Global configuration	on	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	This variable is use	ed only for internal development and testing.	
	Filenames and directory names are case sensitive.		
		nges the setting of the HELPER_CONFIG_FILE environment variable. For more ppendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."	
Related Commands	Command	Description	
	show boot	Displays the settings of the boot environment variables.	

boot manual

Use the **boot manual** global configuration command to enable manually booting the switch during the next boot cycle. Use the **no** form of this command to return to the default setting.

boot manual

no boot manual

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

Defaults Manual booting is disabled.

Command Modes Global configuration

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

Usage Guidelines The next time you reboot the system, the switch is in boot loader mode, which is shown by the *switch:* prompt. To boot the system, use the **boot** boot loader command, and specify the name of the bootable image.

This command changes the setting of the MANUAL_BOOT environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot private-config-file

Use the **boot private-config-file** global configuration command to specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration. Use the **no** form of this command to return to the default setting.

boot private-config-file filename

no boot private-config-file

Syntax Description	filename	The name of the private configuration file.
Defaults	The default configu	uration file is <i>private-config</i> .
Command Modes	Global configuration	on
	Delesse	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
	F '1	
Usage Guidelines	Filenames are case	sensitive.
Examples	This example show	s how to specify the name of the private configuration file to be <i>pconfig</i> :
	Switch(config)# 1	poot private-config-file pconfig
Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot system

Use the **boot system** global configuration command to specify the Cisco IOS image to load during the next boot cycle. Use the **no** form of this command to return to the default setting.

boot system filesystem:/file-url ...

no boot system

Ifile-url The path (directory) and name of a bootable image. Separate image names with a semicolon. Defaults The switch attempts to automatically boot the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image i can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in th original directory. Command Modes Global configuration Command History Release Modification 12.2(25)EX This command was introduced. If you are using the archive download-sw privileged EXEC command to maintain system images, you never need to use the boot system command. The boot system command is automatically manipulate to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."	Syntax Description	filesystem:	Alias for a flash file system. Use flash: for the system board flash device.
variable. If this variable is not set, the switch attempts to load and execute the first executable image i can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in th original directory. Command Modes Global configuration Command History Release Modification 12.2(25)EX This command was introduced. Usage Guidelines Filenames and directory names are case sensitive. If you are using the archive download-sw privileged EXEC command to maintain system images, you never need to use the boot system command. The boot system command is automatically manipulated to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see		lfile-url	
variable. If this variable is not set, the switch attempts to load and execute the first executable image i can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in th original directory. Command Modes Global configuration Command History Release Modification 12.2(25)EX This command was introduced. Usage Guidelines Filenames and directory names are case sensitive. If you are using the archive download-sw privileged EXEC command to maintain system images, you never need to use the boot system command. The boot system command is automatically manipulated to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see	Defaulto	TT	
Command History Release Modification 12.2(25)EX This command was introduced. Usage Guidelines Filenames and directory names are case sensitive. If you are using the archive download-sw privileged EXEC command to maintain system images, you never need to use the boot system command. The boot system command is automatically manipulated to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see	Derauits	variable. If this vari can by performing a of a directory, each	iable is not set, the switch attempts to load and execute the first executable image it a recursive, depth-first search throughout the flash file system. In a depth-first search
12.2(25)EX This command was introduced. Usage Guidelines Filenames and directory names are case sensitive. If you are using the archive download-sw privileged EXEC command to maintain system images, you never need to use the boot system command. The boot system command is automatically manipulated to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see	Command Modes	Global configuratio	n
Usage Guidelines Filenames and directory names are case sensitive. If you are using the archive download-sw privileged EXEC command to maintain system images, you never need to use the boot system command. The boot system command is automatically manipulated to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see	Command History	Release	Modification
If you are using the archive download-sw privileged EXEC command to maintain system images, you never need to use the boot system command. The boot system command is automatically manipulated to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see		12.2(25)EX	This command was introduced.
never need to use the boot system command. The boot system command is automatically manipulated to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see	Usage Guidelines	Filenames and direc	ctory names are case sensitive.
		never need to use th	he boot system command. The boot system command is automatically manipulated
Related Commands Command Description	Related Commands	Command	Description
show boot Displays the settings of the boot environment variables.		show boot	Displays the settings of the boot environment variables.

channel-group

Use the **channel-group** interface configuration command to assign an Ethernet port to an EtherChannel group. Use the **no** form of this command to remove an Ethernet port from an EtherChannel group.

channel-group *channel-group-number* mode {active | {auto [non-silent] | desirable [non-silent] | on} | passive}

no channel-group

PAgP modes:

channel-group channel-group-number mode {auto [non-silent] | {desirable [non-silent]}

LACP modes:

channel-group *channel-group-number* **mode** {**active** | **passive**}

On mode:

channel-group channel-group-number mode on



Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP.) are available only on network node interfaces (NNIs).

Syntax Description	channel-group-number	Specify the channel group number. The range is 1 to 48.
	mode	Specify the EtherChannel mode.
	active	Unconditionally enable LACP
		Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.
	auto	Enable the PAgP only if a PAgP device is detected.
		Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When auto is enabled, silent operation is the default.
	desirable	Unconditionally enable PAgP.
		Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. A channel is formed with another port group in either the desirable or auto mode. When desirable is enabled, silent operation is the default.
	non-silent	(Optional) Use in PAgP mode with the auto or desirable keyword when traffic is expected from the other device.

	on	Enable on mode.
		In on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.
	passive	Enable LACP only if a LACP device is detected.
		Passive mode places a port into a negotiating state in which the port responds to LACP packets it receives but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.
Defaults	No channel groups	are assigned.
	No mode is configu	ured.
Command Modes	Interface configura	tion
Command History	Release	Modification
,	12.2(25)EX	This command was introduced.
	Instead, you can us port-channel interfa already created. If y as the <i>port-channel</i>	al configuration command before assigning a physical port to a channel group. The the channel-group interface configuration command. It automatically creates the ace when the channel group gets its first physical port if the logical interface is not you create the port-channel interface first, the <i>channel-group-number</i> can be the same <i>t-number</i> , or you can use a new number. If you use a new number, the channel-group ally creates a new port channel.
		network interface (UNI), you must use the no shutdown interface configuration e it before using the channel-group command. UNIs are disabled by default. NNIs nult.
	apply to all the phy the physical port af ports in an EtherCh	e an EtherChannel, configuration changes that you make on the port-channel interface viscal ports assigned to the port-channel interface. Configuration changes applied to fect only the port where you apply the configuration. To change the parameters of all hannel, apply configuration commands to the port-channel interface, for example, mands or commands to configure a Layer 2 EtherChannel as a trunk.
	If you do not specif used when the swit packets. A example In this case, runnin However, it allows	fy non-silent with the auto or desirable mode, silent is assumed. The silent mode is ch is connected to a device that is not PAgP-capable and seldom, if ever, sends e of a silent partner is a file server or a packet analyzer that is not generating traffic. g PAgP on a physical port prevents that port from ever becoming operational. PAgP to operate, to attach the port to a channel group, and to use the port for ends of the link cannot be set to silent.
	In the on mode, an port group in the o	EtherChannel exists only when a port group in the on mode is connected to another n mode.

\wedge	
Caution	You should exercise care when setting the mode to on (manual configuration). All ports configured in the on mode are bundled in the same group and are forced to have similar characteristics. If the group is misconfigured, packet loss or spanning-tree loops might occur.
	Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.
Note	PAgP and LACP are available only on NNIs.
	If you set the protocol by using the channel-protocol interface configuration command, the setting is not overridden by the channel-group interface configuration command.
	Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x on an EtherChannel port, an error message appears, and IEEE 802.1x is not enabled.
	Do not configure a secure port as part of an EtherChannel or an EtherChannel port as a secure port.
	For a complete list of configuration guidelines, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.
Examples	This example shows how to configure an EtherChannel. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable :
	Switch# configure terminal Switch(config)# interface range gigabitethernet0/1 -2 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 10 Switch(config-if-range)# channel-group 5 mode desirable Switch(config-if-range)# end
	This example shows how to configure an EtherChannel. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode active :
	Switch# configure terminal Switch(config)# interface range gigabitethernet0/1 -2 Switch(config-if-range)# switchport mode access Switch(config-if-range)# switchport access vlan 10 Switch(config-if-range)# channel-group 5 mode active Switch(config-if-range)# end
	You can verify your settings by entering the show running-config privileged EXEC command.

Related Commands C

Command	Description
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates the port channel.
show etherchannel	Displays EtherChannel information for a channel.
show lacp	Displays LACP channel-group information.
show pagp	Displays PAgP channel-group information.
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.

channel-protocol

Use the **channel-protocol** interface configuration command to restrict the protocol used on a port to manage channeling. Use the **no** form of this command to return to the default setting.

channel-protocol {lacp | pagp}

no channel-protocol

Syntax Description	lacp	Configure an EtherChannel with the Link Aggregation Control Protocol (LACP).
	pagp	Configure an EtherChannel with the Port Aggregation Protocol (PAgP).
Defaults	No protocol is	assigned to the EtherChannel.
Command Modes	Interface confi	guration
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	by using the ch configuration c	
Note	PAgP and LAC	CP are available only on network node interfaces (NNIs).
		user network interface (UNI), you must use the no shutdown interface configuration nable it before using the channel-protocol command. UNIs are disabled by default. NNIs default.
		he channel-group interface configuration command to configure the EtherChannel are channel-group command also can set the mode for the EtherChannel.
	You cannot ena	able both the PAgP and LACP modes on an EtherChannel group.
	PAgP and LAC	CP are not compatible; both ends of a channel must use the same protocol.
Examples	-	shows how to specify LACP as the protocol that manages the EtherChannel:
	-	-if)# channel-protocol lacp
	You can verify privileged EXI	your settings by entering the show etherchannel [<i>channel-group-number</i>] protocol EC command.

Related Commands	Command	Description
	channel-group	Assigns an Ethernet port to an EtherChannel group.
	show etherchannel protocol	Displays protocol information the EtherChannel.

class

Use the **class** policy-map configuration command to specify the name of the class whose policy you want to create or to change or to specify the system default class before you configure a policy and to enter policy-map class configuration mode. Use the **no** form of this command to remove the class from a policy map.

class {class-map-name/ class-default}

no class { class-map-name/ class-default }

Syntax Description	class-map-name	Name of a class map created by using the class-map global configuration command.
	class-default	The system default class. This class matches all unclassified traffic. You cannot create or delete the default class.
Defaults	No policy map classe	s are defined.
Command Modes	Policy-map configura	tion
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines		s <i>class-map-name</i> command in policy-map configuration mode, you must create class-map <i>class-map-name</i> global configuration command. The class
	1 10 14 1 1	
	in the configured clas Use the policy-map g	ass to which traffic is directed if that traffic does not match any of the match criteria s maps. global configuration command to identify the policy map and to enter policy-map
	in the configured clas Use the policy-map g configuration mode. A	ass to which traffic is directed if that traffic does not match any of the match criteria s maps.
	in the configured clas Use the policy-map g configuration mode. <i>A</i> a policy for any existi	ass to which traffic is directed if that traffic does not match any of the match criteria s maps. global configuration command to identify the policy map and to enter policy-map After specifying a policy map, you can configure a policy for new classes or modify
	in the configured clas Use the policy-map g configuration mode. <i>A</i> a policy for any existi An input policy map of	ass to which traffic is directed if that traffic does not match any of the match criteria s maps. global configuration command to identify the policy map and to enter policy-map After specifying a policy map, you can configure a policy for new classes or modify ing classes in that policy map.
	in the configured clas Use the policy-map g configuration mode. <i>A</i> a policy for any existi An input policy map o You attach the policy	ass to which traffic is directed if that traffic does not match any of the match criteria s maps. global configuration command to identify the policy map and to enter policy-map After specifying a policy map, you can configure a policy for new classes or modify ing classes in that policy map. can have a maximum of 32 classes, one of which is class-default . map to a port by using the service-policy interface configuration command. ss command, you enter policy-map class configuration mode, and these
	 in the configured class Use the policy-map ground configuration mode. A a policy for any exists An input policy map of You attach the policy After entering the class bandwidth: spece 	ass to which traffic is directed if that traffic does not match any of the match criteria s maps. global configuration command to identify the policy map and to enter policy-map After specifying a policy map, you can configure a policy for new classes or modify ing classes in that policy map. can have a maximum of 32 classes, one of which is class-default . map to a port by using the service-policy interface configuration command. ss command, you enter policy-map class configuration mode, and these
	 in the configured class Use the policy-map ground configuration mode. A a policy for any existing An input policy map of You attach the policy After entering the class bandwidth: specting formation, see to a section of the sectio	ass to which traffic is directed if that traffic does not match any of the match criteria s maps. global configuration command to identify the policy map and to enter policy-map After specifying a policy map, you can configure a policy for new classes or modify ing classes in that policy map. can have a maximum of 32 classes, one of which is class-default . map to a port by using the service-policy interface configuration command. ss command, you enter policy-map class configuration mode, and these nds are available: ifies the bandwidth allocated for a class belonging to a policy map. For more

- **police**: defines an individual policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** and **police aggregate** (**policy-map** class configuration) policy-map class commands.
- **priority**: sets the strict scheduling priority for this class or, when used with the **police** keyword, sets priority with police. For more information, see the **priority** policy-map class command.
- **queue-limit**: sets the queue maximum threshold for Weighted Tail Drop (WTD). For more information, see the **queue-limit** command.
- service-policy: configures a QoS service policy to attach to a parent policy map for an input or output policy. For more information, see the service-policy (policy-map class configuration) command.
- set: specifies a value to be assigned to the classified traffic. For more information, see the set commands.
- **shape average**: specifies the average traffic shaping rate. For more information, see the **shape average** command.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples This example shows how to create a policy map called *policy1*, define a class *class1*, and enter policy-map class configuration mode to set a criterion for the class.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the show policy-map privileged EXEC command.

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.
	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.

class-map

Use the **class-map** global configuration command to create a class map to be used for matching packets to a specified criteria and to enter class-map configuration mode. Use the **no** form of this command to delete an existing class map.

class-map [match-all | match-any] class-map-name

no class-map [match-all | match-any] class-map-name

Syntax Description	match-all	(Optional) Perform a logical-AND of all matching statements under this class	
		map. Packets must meet all of the match criteria.	
	match-any	(Optional) Perform a logical-OR of the matching statements under this class	
		map. Packets must meet one or more of the match criteria.	
	class-map-name	Name of the class map.	
Defaults	No class maps are defined.		
	If neither the match-all or the match-any keyword is specified, the default is match-all .		
Command Modes	Global configuration		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	Use this command to specify the name of the class for which you want to create or to modify class-map match criteria and to enter class-map configuration mode.		
	The switch supports a maximum of 256 unique class maps.		
	You use the class-map command and class-map configuration mode to define packet classification as part of a globally named service policy applied on a per-port basis. When you configure a class map, you can use one or more match commands to specify match criteria. Packets arriving at either the input or output interface (determined by how you configure the service-policy interface configuration command) are checked against the class-map match criteria to determine if the packet belongs to that class.		
	A match-all class r statements.	nap means that the packet must match all entries and can have no other match	

After you are in class-map configuration mode, these configuration commands are available:

- **description**: describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- exit: exits QoS class-map configuration mode.
- **match**: configures classification criteria. For more information, see the **match** class-map configuration commands.
- **no**: removes a match statement from a class map.

Examples

This example shows how to configure the class map called *class1*. By default, the class map is **match-all** and therefore can contain no other match criteria.

Switch(config)# class-map class1
Switch(config-cmap)# exit

This example shows how to configure a match-any class map with one match criterion, which is an access list called *103*. This class map (matching an ACL) is supported only in an input policy map.

Switch(config) # class-map class2
Switch(config-cmap) # match access-group 103
Switch(config-cmap) # exit

This example shows how to delete the class map *classl*:

Switch(config) # no class-map class1

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Commands	Command	Description
	class	Defines a traffic classification match criteria for the specified class-map name.
	match access-group	Configures the match criteria for a class map on the basis of the specified access control list (ACL)
	match cos	Configures the match criteria for a class map on the basis of the Layer 2 class of service (CoS) marking,
	match ip dscp	Configures the match criteria for a class map on the basis of a specific IPv4 Differentiated Service Code Point (DSCP) value.
	match ip precedence	Configures the match criteria for a class map on the basis of IPv4 precedence values.
	match qos-group	Configures the match criteria for a class map on the basis of a specific quality of service (QoS) group value.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	show class-map	Displays QoS class maps.

clear ip dhcp snooping

Use the **clear ip dhcp snooping** privileged EXEC command to clear the DHCP binding database agent statistics or the DHCP snooping statistics counters.

clear ip dhcp snooping {database statistics | statistics}

Syntax Description	databaseClear the DHCP snooping binding database agent statistics.statistics		
	statistics	Clear the DHCP snooping statistics counter.	
Defaults	No default is	defined.	
Command Modes	Privileged EXEC		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
	12.2(37)SE	The statistics keyword was introduced.	
Usage Guidelines	When you enter the clear ip dhcp snooping database statistics command, the switch does not update the entries in the binding database and in the binding file before clearing the statistics.		
Examples	This example shows how to clear the DHCP snooping binding database agent statistics:		
	Switch# clear ip dhcp snooping database statistics		
	You can verify that the statistics were cleared by entering the show ip dhcp snooping database privileged EXEC command.		
	This example shows how to clear the DHCP snooping statistics counters:		
	Switch# clear ip dhcp snooping statistics		
	You can verify that the statistics were cleared by entering the show ip dhcp snooping statistics user EXEC command.		

Related Commands Co

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 binding	Displays the status of DHCP snooping database agent.
show ip dhcp snooping database	Displays the DHCP snooping binding database agent statistics.
show ip dhcp snooping statistics	Displays the DHCP snooping statistics.

clear lacp

Use the **clear lacp** privileged EXEC command to clear Link Aggregation Control Protocol (LACP) channel-group counters.

clear lacp {channel-group-number counters | counters}

۵, Note

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

Syntax Description	channel-group-number	(Optional) Channel group number. The range is 1 to 48.
	counters	Clear traffic counters.
Defaults	No default is defined.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	You can clear all counter	s by using the clear lacp counters command, or you can clear only the counters l group by using the clear lacp <i>channel-group-number</i> counters command.
Usage Guidelines	You can clear all counter for the specified channel	is by using the clear lacp counters command, or you can clear only the counters I group by using the clear lacp <i>channel-group-number</i> counters command.
Usage Guidelines Examples	You can clear all counter for the specified channel	rs by using the clear lacp counters command, or you can clear only the counters I group by using the clear lacp <i>channel-group-number</i> counters command. w to clear all channel-group information:
	You can clear all counter for the specified channel This example shows how Switch# clear lacp con	rs by using the clear lacp counters command, or you can clear only the counters I group by using the clear lacp <i>channel-group-number</i> counters command. w to clear all channel-group information:
	You can clear all counter for the specified channel This example shows how Switch# clear lacp con	The set of
	You can clear all counter for the specified channel This example shows how Switch# clear lacp co This example shows how Switch# clear lacp 4	The set of the show lacp counters for group 4: show lacp 4 show lacp 4
	You can clear all counter for the specified channel This example shows how Switch# clear lacp co This example shows how Switch# clear lacp 4 o You can verify that the in	The set of the show lacp counters for the show lacp 4

clear mac address-table

Use the **clear mac address-table** privileged EXEC command to delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN. This command also clears the MAC address notification global counters.

clear mac address-table {dynamic [address mac-addr | interface interface-id | vlan vlan-id] |
 notification}

Syntax Description	dynamic	Delete all dyr	amic MAC addresses.
	dynamic address <i>mac-addr</i>	(Optional) De	lete the specified dynamic MAC address.
	dynamic interface <i>interface-id</i>	(Optional) De or port channe	lete all dynamic MAC addresses on the specified physical port el.
	dynamic vlan vlan-id	(Optional) De range is 1 to 4	lete all dynamic MAC addresses for the specified VLAN. The 096.
	notification	Clear the noti	fications in the history table and reset the counters.
Defaults	No default is defined.		
Command Modes	Privileged EXEC		
Command History	Release	Modification	
	12.2(25)EX	This comman	d was introduced.
Examples	This example shows how to remove a specific MAC address from the dynamic address table: Switch# clear mac address-table dynamic address 0008.0070.0007		
	You can verify that the in EXEC command.	nformation was	deleted by entering the show mac address-table privileged
Related Commands	Command		Description
	mac address-table noti	fication	Enables the MAC address notification feature.
	show mac address-tabl	e	Displays the MAC address table static and dynamic entries.
	show mac address-tabl show mac address-tabl	-	Displays the MAC address table static and dynamic entries. Displays the MAC address notification settings for all interfaces or the specified interface.

clear pagp

Use the **clear pagp** privileged EXEC command to clear Port Aggregation Protocol (PAgP) channel-group information.

clear pagp {channel-group-number counters | counters}

۵, Note

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

Syntax Description	channel-group-number	(Optional) Channel group number. The range is 1 to 48.
	counters	Clear traffic counters.
Defaults	No default is defined.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines		s by using the clear pagp counters command, or you can clear only the counters l group by using the clear pagp <i>channel-group-number</i> counters command.
Examples	This example shows how	v to clear all channel-group information:
	Switch# clear pagp co	unters
	This example shows how	v to clear PAgP traffic counters for group 10:
	Switch# clear pagp 10	counters
	You can verify that infor	rmation was deleted by entering the show pagp privileged EXEC command.
Related Commands	Command	Description
	show pagp	Displays PAgP channel-group information.

clear policer cpu uni counters

Use the **clear policer cpu uni counters** privileged EXEC command to clear control-plane policer statistics. The control-plane policer drops or rate-limits control packets from user network interfaces (UNIs) to protect the CPU from overload.

clear policer cpu uni counters {classification | drop}

Syntax Description	classification	Clear control-pla	ane policer classification counters that maintain statistics by feature.
	drop	Clear all frame of	drop statistics maintained by the control-plane policer.
Command Default	No default is de	efined.	
Command Modes	User EXEC		
Command History	Release	Modifi	cation
	12.2(25)EX	This co	ommand was introduced.
Usage Guidelines	You can use thi	s command to cle	ar statistics maintained per feature or statistics about dropped frames.
		-	policer cpu classification or show policer cpu uni drop command to frames before and after you use the clear command.
Related Commands	Command		Description
	show platform classification	ı policer cpu	Displays CPU policer statistics per feature.
		pu uni	Displays CPU policer information for the switch.

clear port-security

Use the **clear port-security** privileged EXEC command to delete from the MAC address table all secure addresses or all secure addresses of a specific type (configured, dynamic, or sticky) on the switch or on an interface.

clear port-security {**all** | **configured** | **dynamic** | **sticky**} [[**address** *mac-addr* | **interface** *interface-id*] [**vlan** {*vlan-id* | {**access** | **voice**}]]]

Syntax Description	all	Delete all secure MAC addresses.		
	configured	Delete configured secure MAC addresses.		
	dynamic	Delete secure MAC addresses auto-learned by hardware.		
	sticky	Delete secure MAC addresses, either auto-learned or configured.		
	address mac-addr	(Optional) Delete the specified dynamic secure MAC address.		
	interface interface-id	(Optional) Delete all the dynamic secure MAC addresses on the specified physical port or VLAN.		
	vlan	(Optional) Delete the specified secure MAC address from the specified VLAN. Enter one of these options after you enter the vlan keyword:		
		• <i>vlan-id</i> —On a trunk port, specify the VLAN ID of the VLAN on which this address should be cleared.		
		• access —On an access port, clear the specified secure MAC address on the access VLAN.		
Defaults	No default is defined.			
Command Modes	Privileged EXEC			
Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
Examples	-	w to clear all secure addresses from the MAC address table:		
	Switch# clear port-security all			
	This example shows how to remove a specific configured secure address from the MAC address table: Switch# clear port-security configured address 0008.0070.0007			
	This example shows how to remove all the dynamic secure addresses learned on a specific interface:			
	-			
	-	w to remove all the dynamic secure addresses learned on a specific interface: curity dynamic interface gigabitethernet0/1		

You can verify that the information was deleted by entering the **show port-security** privileged EXEC command.

Related Commands	Command	Description
	switchport port-security	Enables port security on an interface.
	switchport port-security mac-address mac-address	Configures secure MAC addresses.
	switchport port-security maximum <i>value</i>	Configures a maximum number of secure MAC addresses on a secure interface.
	show port-security	Displays the port security settings defined for an interface or for the switch.

clear spanning-tree counters

Use the **clear spanning-tree counters** privileged EXEC command to clear the spanning-tree counters.

clear spanning-tree counters [interface interface-id]

Syntax Description	interface interface-id	(Optional) Clear all spanning-tree counters on the specified interface. Valid interfaces include physical network node interfaces (NNIs), VLANs, and 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 network interfaces (UNIs). Though visible in the command-line help, the command has no effect on UNIs.
Defaults	No default is defined.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	If the <i>interface-id</i> is not	t specified, spanning-tree counters are cleared for all NNIs.
Examples	This example shows ho	w to clear spanning-tree counters for all NNIs:
	Switch# clear spannir	ng-tree counters
Related Commands	Command	Description
	show spanning-tree	Displays spanning-tree state information.

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches) on all spanning-tree interfaces or on the specified interface.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Syntax Description	interface interface-id	(Optional) Restart the protocol migration process on the specified interface. Valid interfaces include physical network node interfaces (NNIs), VLANs, and 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 network interfaces (UNIs). Though visible in the command-line help, the command has no effect on UNIs.
Defaults	No default is defined.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	Spanning Tree Protocol (interoperate with legacy 1 legacy IEEE 802.1D com it sends only IEEE 802.1 that a port is at the bound associated with a differen However, the switch does receives IEEE 802.1D BF	id per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple MSTP) supports a built-in protocol migration mechanism that enables it to IEEE 802.1D switches. If a rapid-PVST+ switch or an MSTP switch receives a figuration bridge protocol data unit (BPDU) with the protocol version set to 0, D BPDUs on that port. A multiple spanning-tree (MST) switch can also detect dary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) at region, or a rapid spanning-tree (RST) BPDU (Version 2). The not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer PDUs. It cannot learn whether the legacy switch has been removed from the link is the designated switch. Use the clear spanning-tree detected-protocols n.
Examples	-	to restart the protocol migration process on a port: -tree detected-protocols interface gigabitethernet0/1

Related Commands	Command	Description
	show spanning-tree	Displays spanning-tree state information.
	spanning-tree link-type	Overrides the default link-type setting and enables rapid spanning-tree transitions to the forwarding state.

clear vmps statistics

Use the **clear vmps statistics** privileged EXEC command to clear the statistics maintained by the VLAN Query Protocol (VQP) client.

clear vmps statistics

Syntax Description	This command has no a	arguments or keywords.
Defaults	No default is defined.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Examples	This example shows ho Switch# clear vmps st	w to clear VLAN Membership Policy Server (VMPS) statistics:
	You can verify that info command.	ormation was deleted by entering the show vmps statistics privileged EXEC
Related Commands	Command	Description
	show vmps	Displays the VQP version, reconfirmation interval, retry count, VMPS IP addresses, and the current and primary servers.

conform-action

Use the **conform-action** policy-map class police configuration command to set multiple actions for a policy-map class for packets that conform to the committed information rate (CIR). Use the **no** form of this command to cancel the action or return to the default action.

- conform-action {set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit]}
- **no conform-action** {set-cos-transmit {*new-cos-value* | [cos | dscp | precedence] [table *table-map name*]} | set-dscp-transmit {*new-dscp-value* | [cos | dscp | precedence] [table *table-map name*]} | set-prec-transmit {*new-precedence-value* | [cos | dscp | precedence] [table *table-map name*]} | set-qos-transmit *qos-group-value* | transmit]}

yntax Description	set-cos-transmit new-cos-value	Set a new class of service (CoS) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.
	set-dscp-transmit new-dscp-value	Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DCSP value is 0 to 63.
	set-prec-transmit new-precedence-value	Set a new IP precedence value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.
	set-qos-transmit <i>qos-group-value</i>	Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new QoS value is 0 to 99.
	cos	(Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
	dscp	(Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
	precedence	(Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
	table table-map name	(Optional) Used in conjunction with the preceding <i>from-type</i> keyword. Specify the table map to be used for the enhanced packet marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i> parameter of the action using this table map.
	transmit	(Optional) Send the packet unmodified.

Defaults

The default conform action is to send the packet.

Command Modes Policy-map class police configuration

police

show policy-map

Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
	12.2(25)SEG	Increased support for configuring conform-action marking. See "Usage Guidelines."	
Usage Guidelines	Beginning with Cisco IOS release 12.2(25)SEG, you can configure conform-action marking using enhanced packet marking, which provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. This release also added support for the ability to mark multiple QoS parameters for the same class and configure conromf0action marking and exceed-action marking simultaneously.		
	Access policy-map class police configuration mode by entering the police policy-map class command. See the police command for more information.		
	Use this command to	o set one or more conform actions for a traffic class.	
Examples	information rate of 2	how configure multiple conform actions in a policy map that sets a committed 23000 bits per second (bps) and a conform burst rate of 10000 bps. The policy map nform actions (for DSCP and for Layer 2 CoS) and an exceed action.	
	Switch (config-pmag Switch (config-pmag Switch (config-pmag	<pre>b)# class cos-set-1 b-c)# police cir 23000 bc 10000 b-c-police)# conform-action set-dscp-transmit 48 b-c-police)# conform-action set-cos-transmit 5 b-c-police)# exceed-action drop</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.	
	exceed-action	Defines the action to take on traffic that exceeds the CIR.	
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.	

Defines a policer for classified traffic.

Displays QoS policy maps.

define interface-range

Use the **define interface-range** global configuration command to create an interface-range macro. Use the **no** form of this command to delete the defined macro.

define interface-range macro-name interface-range

no define interface-range macro-name interface-range

Syntax Description		Name of the interface-range macro; up to 32 characters.	
Syntax Description	macro-name	Interface range; for valid values for interface ranges, see "Usage Guidelines."	
	interface-range	Interface range, for valid values for interface ranges, see Osage Outdennes.	
Defaults	This command ha	s no default setting.	
Command Modes	Global configurati	ion	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	The macro name is a 32-character maximum character string.		
	A macro can contain up to five ranges.		
	All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs, but you can combine multiple interface types in a macro.		
	 When entering the <i>interface-range</i>, use this format: type {first-interface} - {last-interface} 		
	 You must add a space between the first interface number and the hyphen when entering an <i>interface-range</i>. For example, gigabitethernet 0/1 - 2 is a valid range; gigabitethernet 0/1-2 is not a valid range 		
	Valid values for ty	ppe and interface:	
	• vlan vlan-id,	where <i>vlan-id</i> is from 1 to 4094	
	VLAN interfaces must have been configured with the interface vlan command (the show running-config privileged EXEC command displays the configured VLAN interfaces). VLAN interfaces not displayed by the show running-config command cannot be used in <i>interface-ranges</i> .		
	• port-channel	port-channel-number, where port-channel-number is from 1 to 48	
	• fastethernet	module/{first port} - {last port}	
	• gigabitetherr	net module/{first port} - {last port}	

For physical interfaces:

- module is always 0.
- the range is *type* **0**/*number number* (for example, **gigabitethernet 0**/**1 2**).

When you define a range, you must enter a space before the hyphen (-), for example:

gigabitethernet0/1 - 2

You can also enter multiple ranges. When you define multiple ranges, you must enter a space after the first entry before the comma (,). The space after the comma is optional, for example:

fastethernet0/3, gigabitethernet0/1 - 2

fastethernet0/3 -4, gigabitethernet0/1 - 2

Examples

This example shows how to create a multiple-interface macro:

Switch(config)# define interface-range macrol fastethernet0/1 - 2, gigabitethernet0/1 - 2

Related Commands

Command	Description	
interface range	Executes a command on multiple ports at the same time.	
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. 	

delete

Use the **delete** privileged EXEC command to delete a file or directory on the flash memory device.

delete [/force] [/recursive] filesystem:/file-url

Syntax Description	/force	(Optional) Suppress the prompt that confirms the deletion.			
ojinan Doconpriori		(Optional) Delete the named directory and all subdirectories and the files contained in			
		it.			
	filesystem:	Alias for a flash file system.			
		The syntax for the local flash file system: flash:			
	lfile-url	The path (directory) and filename to delete.			
Command Modes	Privileged EXEC				
Command History	Release	Modification			
	12.2(25)EX	This command was introduced.			
	If you use the / recursive keyword without the / force keyword, you are prompted to confirm the deletion of every file. The prompting behavior depends on the setting of the file prompt global configuration command. By default, the switch prompts for confirmation on destructive file operations. For more information about this command, see the <i>Cisco IOS Command Reference for Release 12.1</i> .				
Examples	This example shows how to remove the directory that contains the old software image after a successful download of a new image:				
	Switch# delete /force /recursive flash:/old-image				
	You can verify that the directory was removed by entering the dir <i>filesystem</i> : privileged EXEC command.				
Related Commands	Command	Description			
	archive downloa	ad-sw Downloads a new image to the switch and overwrites or keeps the existing			

deny (MAC access-list configuration)

Use the **deny** MAC access-list configuration command to prevent non-IP traffic from being forwarded if the conditions are matched. Use the **no** form of this command to remove a deny condition from the named MAC access list.

- {deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | cos cos | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask |mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
- no {deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | cos cos | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]

Syntax Description	any	Keyword to specify to deny any source or destination MAC address.
	host <i>src MAC-addr</i> <i>src-MAC-addr mask</i>	Define a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
	host <i>dst-MAC-addr</i> <i>dst-MAC-addr</i> mask	Define a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
	type mask	(Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.
		The type is 0 to 65535, specified in hexadecimal.
		The <i>mask</i> is a mask of <i>don't care</i> bits applied to the Ethertype before testing for a match.
	aarp	(Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
	amber	(Optional) Select EtherType DEC-Amber.
	COS COS	(Optional) Select a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the cos option is configured.
	dec-spanning	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
	decnet-iv	(Optional) Select EtherType DECnet Phase IV protocol.
	diagnostic	(Optional) Select EtherType DEC-Diagnostic.
	dsm	(Optional) Select EtherType DEC-DSM.
	etype-6000	(Optional) Select EtherType 0x6000.
	etype-8042	(Optional) Select EtherType 0x8042.
	lat	(Optional) Select EtherType DEC-LAT.
	lavc-sca	(Optional) Select EtherType DEC-LAVC-SCA.

lsap lsap-number mask	(Optional) Use the LSAP number (0 to 65535) of a packet with IEEE 802.2 encapsulation to identify the protocol of the packet.	
	<i>mask</i> is a mask of <i>don't care</i> bits applied to the LSAP number before testing for a match.	
mop-console	(Optional) Select EtherType DEC-MOP Remote Console.	
mop-dump	(Optional) Select EtherType DEC-MOP Dump.	
msdos	(Optional) Select EtherType DEC-MSDOS.	
mumps	(Optional) Select EtherType DEC-MUMPS.	
netbios	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).	
vines-echo(Optional) Select EtherType Virtual Integrated Network Service (' Echo from Banyan Systems.		
vines-ip (Optional) Select EtherType VINES IP.		
xns-idp	(Optional) Select EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal.	

Note

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in Table 2-1.

Table 2-1 IPX Filtering Criteria

IPX Encapsulation Type		
Cisco IOS Name	Novel Name	Filter Criterion
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

Defaults This command has no defaults. However; the default action for a MAC-named ACL is to deny.

Command ModesMAC-access list configuration

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

show access-lists

	mac access-list extended permit (MAC access-list configuration)	Creates an access list based on MAC addresses for non-IP traffic. Permits non-IP traffic to be forwarded if conditions are matched.	
Related Commands	Command	Description	
	You can verify your settings by	y entering the show access-lists privileged EXEC command.	
	Switch(config-ext-macl)# deny any 0x4321 0		
	Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000 netbios. This example denies all packets with Ethertype 0x4321:		
	L.	move the deny condition from the named MAC extended access list:	
	Switch(config-ext-macl)# de	eny any host 00c0.00a0.03fa netbios.	
Examples	This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.		
	this release.		
Note	For more information about na	med MAC extended access lists, see the software configuration guide for	
	When an access control entry (ACE) is added to an access control list, an implied deny-any-any condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.		
	If you use the host keyword, yo must enter an address mask.	ou cannot enter an address mask; if you do not use the host keyword, you	
Usage Guidelines	You enter MAC-access list configuration mode by using the mac access-list extended global configuration command.		

Displays access control lists configured on a switch.

dot1x default

Use the **dot1x default** interface configuration command to reset the configurable IEEE 802.1x parameters to their default values.

dot1x default

Syntax Description	This command has no arguments or ke	eywords.	
Defaults	These are the default values:		
	• The per-port IEEE 802.1x protoco	el enable state is disabled (force-authorized).	
	• The number of seconds between r	e-authentication attempts is 3600 seconds.	
	• The periodic re-authentication is	lisabled.	
	• The quiet period is 60 seconds.		
	• The retransmission time is 30 sec	onds.	
	• The maximum retransmission nur	nber is 2 times.	
	• The host mode is single host.		
	• The client timeout period is 30 se	conds.	
	• The authentication server timeout period is 30 seconds.		
Command Modes	• The authentication server timeout Interface configuration	period is 30 seconds.	
	Interface configuration	-	
	Interface configuration Release Modificatio	-	
Command History	Interface configurationReleaseModification12.2(25)EXThis command	n nd was introduced.	
Command History	Interface configurationReleaseModification12.2(25)EXThis command	1	
Command History	Interface configurationReleaseModification12.2(25)EXThis commandThis example shows how to reset the or Switch(config-if)# dot1x default	n nd was introduced.	
Command Modes Command History Examples	Interface configurationReleaseModification12.2(25)EXThis commandThis example shows how to reset the of Switch(config-if)# dot1x defaultYou can verify your settings by entering	n und was introduced. configurable IEEE 802.1x parameters on a port:	

dot1x host-mode

Use the **dot1x host-mode** interface configuration command to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**. Use the **no** form of this command to return to the default setting.

dot1x host-mode {multi-host | single-host}

no dot1x host-mode [multi-host | single-host]

Syntax Description	multi-host	Enable multiple	-hosts mode on the switch.
	single-host	Enable single-ho	ost mode on the switch.
Defaults	The default is single-host mode.		
Command Modes	Interface configuration		
Command History	Release	Modification	
	12.2(25)EX	This commar	nd was introduced.
Usage Guidelines	Use this command to limit an IEEE 802.1x-enabled port to a single client or to attach multiple clients to an IEEE 802.1x-enabled port. In multiple-hosts mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.		
	-	is command, make su the specified port.	re that the dot1x port-control interface configuration command
Examples	This example shows how to enable IEEE 802.1x globally, to enable IEEE 802.1x on a port, and to enable multiple-hosts mode:		
	Switch(config)# dotlx system-auth-control Switch(config)# interface gigabitethernet0/1 Switch(config-if)# dotlx port-control auto Switch(config-if)# dotlx host-mode multi-host		
	You can verify yo command.	our settings by entering	g the show dot1x [interface <i>interface-id</i>] privileged EXEC
Related Commands	Command		Description
	show dot1x [inte	erface interface-id]	Displays IEEE 802.1x status for the specified port.

dot1x initialize

Use the **dot1x initialize** privileged EXEC command to manually return the specified IEEE 802.1x-enabled port to an unauthorized state before initiating a new authentication session on the port.

dot1x initialize interface interface-id

Syntax Description	interface interface-id	Port to be initialized.
Defaults	There is no default setting	<u>.</u>
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines		alize the IEEE 802.1x state machines and to set up a fresh environment for enter this command, the port status becomes unauthorized. is command.
Examples	This example shows how	to manually initialize a port:
-	Switch# dot1x initializ	ze interface gigabitethernet0/2
	You can verify the unauth privileged EXEC commar	orized port status by entering the show dot1x [interface <i>interface-id</i>] nd.
Related Commands	Command	Description
	<pre>show dot1x [interface in</pre>	<i>terface-id</i>] Displays IEEE 802.1x status for the specified port.

dot1x max-reauth-req

Use the **dot1x max-reauth-req** interface configuration command to set the maximum number of times that the switch restarts the authentication process before a port transitions to the unauthorized state. Use the **no** form of this command to return to the default setting.

dot1x max-reauth-req count

no dot1x max-reauth-req

Syntax Description		umber of times that the switch restarts the authentication process before the ort transitions to the unauthorized state. The range is 1 to 10.	
Defaults	The default is 2 times.		
Command Modes	Interface configuration		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	•	fault value of this command only to adjust for unusual circumstances such as c behavioral problems with certain clients and authentication servers.	
Examples	This example shows how to set 4 as the number of times that the switch restarts the authentication process before the port transitions to the unauthorized state:		
	Switch(config-if)# dot1x max-reauth-req 4		
	You can verify your settin command.	ngs by entering the show dot1x [interface <i>interface-id</i>] privileged EXEC	
Related Commands	Command	Description	
	dot1x max-req	Sets the maximum number of times that the switch forwards an EAP frame (assuming that no response is received) to the authentication server before restarting the authentication process.	
	dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request.	
	<pre>show dot1x [interface interface-id]</pre>	Displays IEEE 802.1x status for the specified port.	

dot1x max-req

Use the **dot1x max-req** interface configuration command to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP) frame from the authentication server (assuming that no response is received) to the client before restarting the authentication process. Use the **no** form of this command to return to the default setting.

dot1x max-req count

no dot1x max-req

Syntax Description		Number of times that the switch resends an EAP frame from the authentication server before restarting the authentication process. The range is 1 to 10.	
Defaults	The default is 2 times.		
Command Modes	Interface configuration		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines Examples	unreliable links or spec. This example shows ho	default value of this command only to adjust for unusual circumstances such as ific behavioral problems with certain clients and authentication servers. we to set 5 as the number of times that the switch sends an EAP frame from the efore restarting the authentication process:	
	Switch(config-if)# dot1x max-req 5		
	You can verify your set command.	tings by entering the show dot1x [interface <i>interface-id</i>] privileged EXEC	
Related Commands	Command	Description	
	dot1x timeout tx-perio	od Sets the number of seconds that the switch waits for a response to an	
		EAP-request/identity frame from the client before resending the request.	
	<pre>show dot1x [interface interface-id]</pre>		

dot1x port-control

Use the **dot1x port-control** interface configuration command to enable manual control of the authorization state of the port. Use the **no** form of this command to return to the default setting.

 $dot1x \ port-control \ \{ auto \mid force-authorized \mid force-unauthorized \}$

no dot1x port-control

Syntax Description	auto	Enable IEEE 802.1x authentication on the port and cause the port to change to the authorized or unauthorized state based on the IEEE 802.1x authentication exchange between the switch and the client.	
	force-authorized	Disable IEEE 802.1x authentication on the port and cause the port to change to the authorized state without an authentication exchange. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client.	
	force-unauthorized	Deny all access through this port by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.	
Defaults	The default is force-a	uthorized.	
Command Modes	Interface configuration		
Command History	Release	Modification	
Command History	Release 12.2(25)EX	Modification This command was introduced.	
Command History Usage Guidelines	12.2(25)EX You must globally end		
	12.2(25)EX You must globally ena configuration command	This command was introduced. able IEEE 802.1x on the switch by using the dot1x system-auth-control global	
	12.2(25)EX You must globally ena configuration commany You can use the auto • Trunk port—If you IEEE 802.1x is not	This command was introduced. able IEEE 802.1x on the switch by using the dot1x system-auth-control global and before enabling IEEE 802.1x on a specific port.	

	EtherChannel as an IEEE 802.1x pe an error message appears, and IEEF	
	IEEE 802.1x on a port that is a SPAN	d Remote SPAN (RSPAN) destination ports—You can enable N or RSPAN destination port. However, IEEE 802.1x is disabled or RSPAN destination. You can enable IEEE 802.1x on a SPAN
		switch, use the no dot1x system-auth-control global E 802.1x on a specific port, use the no dot1x port-control
Examples	This example shows how to enable IEE Switch(config)# interface gigabitet Switch(config-if)# dot1x port-contr You can verify your settings by entering command.	hernet0/1
Related Commands	Command	Description
	<pre>show dot1x [interface interface-id]</pre>	Displays IEEE 802.1x status for the specified port.

dot1x re-authenticate

Use the **dot1x re-authenticate** privileged EXEC command to manually initiate a re-authentication of the specified IEEE 802.1x-enabled port.

dot1x re-authenticate interface interface-id

Syntax Description	interface interface-id	Module and port number of the interface to re-authenticate.
Defaults	There is no default settin	g.
Command Modes	Privileged EXEC	
Command History	Release 12.2(25)EX	Modification This command was introduced.
Usage Guidelines	You can use this command to re-authenticate a client without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic re-authentication.	
Examples	This example shows how to manually re-authenticate the device connected to a port: Switch# dotlx re-authenticate interface gigabitethernet0/1	

dot1x reauthentication

Use the **dot1x reauthentication** interface configuration command to enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

dot1x reauthentication

no dot1x reauthentication

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

- Defaults Periodic re-authentication is disabled.
- Command Modes Interface configuration

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

Usage Guidelines You configure the amount of time between periodic re-authentication attempts by using the dot1x timeout reauth-period interface configuration command.

Examples This example shows how to disable periodic re-authentication of the client:

Switch(config-if) # no dot1x reauthentication

This example shows how to enable periodic re-authentication and to set the number of seconds between re-authentication attempts to 4000 seconds:

Switch(config-if)# dotlx reauthentication
Switch(config-if)# dotlx timeout reauth-period 4000

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands	Command	Description
	dot1x timeout reauth-period	Sets the number of seconds between re-authentication attempts.
	<pre>show dot1x [interface interface-id]</pre>	Displays IEEE 802.1x status for the specified port.

Enables manual control of the authorization state of the port.

Displays IEEE 802.1x status for the specified port.

Related Commands	Command Description
	You can verify your settings by entering the show dot1x [interface <i>interface-id</i>] privileged EXEC command.
Examples	This example shows how to globally enable IEEE 802.1x on a switch: Switch(config)# dot1x system-auth-control
	Before globally enabling IEEE 802.1x on a switch, remove the EtherChannel configuration from the interfaces on which IEEE 802.1x and EtherChannel are configured.
	authentieution methods to be queried to authentieute a user.

Modification

authentication methods to be queried to authenticate a user.

This command was introduced.

You must enable authentication, authorization, and accounting (AAA) and specify the authentication

method list before globally enabling IEEE 802.1x. A method list describes the sequence and

dot1x system-auth-control

Syntax Description

Command Modes

Command History

Usage Guidelines

Defaults

Use the **dot1x system-auth-control** global configuration command to globally enable IEEE 802.1x. Use the **no** form of this command to return to the default setting.

dot1x system-auth-control

IEEE 802.1x is disabled.

Global configuration

dot1x port-control show dot1x [interface

interface-id]

Release

12.2(25)EX

no dot1x system-auth-control

This command has no arguments or keywords.

dot1x system-auth-control

dot1x timeout

Use the **dot1x timeout** interface configuration command to set IEEE 802.1x timers. Use the **no** form of this command to return to the default setting.

dot1x timeout {quiet-period seconds | reauth-period seconds | server-timeout seconds |
 supp-timeout seconds | tx-period seconds}

no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}

Syntax Description	quiet-period seconds	Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535.		
	reauth-period seconds	Number of seconds between re-authentication attempts. The range is 1 to 65535.		
	server-timeout seconds	Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server. The range is 30 to 65535.		
	supp-timeout seconds	Number of seconds that the switch waits for the retransmission of packets by the switch to the IEEE 802.1x client. The range is 30 to 65535.		
	tx-period seconds	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 15 to 65535.		
Defaults	These are the default setti	ings:		
	reauth-period is 3600 seconds.			
	quiet-period is 60 seconds.			
	tx-period is 30 seconds.			
	supp-timeout is 30 seconds.			
	server-timeout is 30 seco	onds.		
Command Modes	Interface configuration			
Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
Usage Guidelines	You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.			
	The dot1x timeout reauth-period interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the dot1x reauthentication interface configuration command.			
	• • •	he switch does not accept or initiate any authentication requests. If you want se time to the user, enter a number smaller than the default.		

Examples This example shows how to enable periodic re-authentication and to set 4000 as the number of seconds between re-authentication attempts: Switch(config-if)# dot1x reauthentication Switch(config-if) # dot1x timeout reauth-period 4000 This example shows how to set 30 seconds as the quiet time on the switch: Switch(config-if)# dot1x timeout quiet-period 30 This example shows how to set 45 seconds as the switch-to-authentication server retransmission time: Switch(config) # dot1x timeout server-timeout 45 This example shows how to set 45 seconds as the switch-to-client retransmission time for the EAP request frame: Switch(config-if) # dot1x timeout supp-timeout 45 This example shows how to set 60 as the number of seconds to wait for a response to an EAP-request/identity frame from the client before re-transmitting the request: Switch(config-if) # dot1x timeout tx-period 60 You can verify your settings by entering the **show dot1x** privileged EXEC command.

Related Commands	Command	Description
	dot1x max-req	Sets the maximum number of times that the switch sends an
		EAP-request/identity frame before restarting the authentication process.
	dot1x reauthentication	Enables periodic re-authentication of the client.
	show dot1x	Displays IEEE 802.1x status for all ports.

duplex

Use the **duplex** interface configuration command to specify the duplex mode of operation for a port. Use the **no** form of this command to return the port to its default value.

duplex {auto | full | half}

no duplex

Syntax Description	auto	Enable automatic duplex configuration; port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.	
	full	Enable full-duplex mode.	
	half	Enable half-duplex mode (only for interfaces operating at 10 Mbps or 100 Mbps). You cannot configure half-duplex mode for interfaces operating at 1000 Mbps or 10,000 Mbps.	
Defaults	The default is au pluggable (SFP)	to for Fast Ethernet and Gigabit Ethernet ports and for 1000BASE-T small form-factor modules.	
	The default is ha	alf for 100BASE-FX MMF SFP modules.	
Command Modes	Interface configu	uration	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines		s only available when a 1000BASE-T SFP module or a 100BASE-FX MMF SFP module dule slot. All other SFP modules operate only in full-duplex mode.	
	When a 1000BASE-T SFP module is in the SFP module slot, you can configure duplex mode to auto or full .		
	When a 100BASE-FX MMF SFP module is in the SFP module slot, you can configure duplex mode to half or full . Although the auto keyword is available, it puts the interface in half-duplex mode (the default) because the 100BASE-FX MMF SFP module does not support autonegotiation.		
	Certain ports can be configured to be either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached.		
		For Fast Ethernet ports, setting the port to auto has the same effect as specifying half if the attached device does not autonegotiate the duplex parameter.	
		ernet ports, setting the port to auto has the same effect as specifying full if the attached autonegotiate the duplex parameter.	

	connecte	Half-duplex mode is supported on Gigabit Ethernet interfaces if duplex mode is auto and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.		
	If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do use the auto setting on the supported side.			
	If the speed is set to auto , the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.			
	You can configure the duplex setting when the speed is set to auto .			
<u></u> Caution	Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.			
Note	For guidelines on setting the switch speed and duplex parameters, see the software configurat for this release.			
Examples	This example shows how to configure an interface for full duplex operation:			
	Switch(config)# interface gigabitethernet0/1 Switch(config-if)# duplex full			
	Switch(config-i	I)# duplex full		
		our setting by entering the show interfaces privileged EXEC command.		
Related Commands				
Related Commands	You can verify y	our setting by entering the show interfaces privileged EXEC command. Description		

errdisable detect cause

Use the **errdisable detect cause** global configuration command to enable error-disabled detection for a specific cause or all causes. Use the **no** form of this command to disable the error-disabled detection feature.

errdisable detect cause {all | dhcp-rate-limit | gbic-invalid | link-flap | loopback | pagp-flap }

no errdisable detect cause {all | dhcp-rate-limit | gbic-invalid | link-flap | pagp-flap}

Cumtou Decerintian	- 11	Partite same later ("and from the same the life same		
Syntax Description	all	Enable error detection for all error-disable causes.		
	dhcp-rate-limit	· ·		
	gbic-invalid	Enable error detection for an invalid Gigabit Interface Converter (GBIC) module.		
		Note This error refers to an invalid small form-factor pluggable (SFP) module.		
	link-flap	Enable error detection for link-state flapping.		
	loopback	Enable error detection for detected loopbacks.		
	pagp-flap	Enable error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.		
Note	Though visible in the command-line help string, the arp-inspection keyword is not supported.			
Command Modes	Global configuration	Dn		
Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
Usage Guidelines	A cause (all , dhcp-rate-limit , and so forth) is the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state, an operational state that is similar to a link-down state. If you set a recovery mechanism for the cause by entering the errdisable recovery global configuration command for the cause, the interface is brought out of the error-disabled state and allowed to retry the			
	operation when all	causes have timed out. If you do not set a recovery mechanism, you must enter the no shutdown commands to manually recover an interface from the		
Examples	This example show	s how to enable error-disabled detection for the link-flap error-disabled cause:		

Switch(config)# errdisable detect cause link-flap

You can verify your setting by entering the show errdisable detect privileged EXEC command.

Related Commands	Command	Description
	show errdisable detect	Displays errdisable detection information.
	show interfaces status err-disabled	Displays interface status or a list of interfaces in the error-disabled state.

I

errdisable recovery

Use the **errdisable recovery** global configuration command to configure the recover mechanism variables. Use the **no** form of this command to return to the default setting.

- errdisable recovery {cause {all | bpduguard | channel-misconfig | dhcp-rate-limit | gbic-invalid | link-flap | loopback | pagp-flap | psecure-violation | security-violation | udld |unicast-flood | vmps} | {interval interval}
- no errdisable recovery {cause {all | bpduguard | channel-misconfig | dhcp-rate-limit | gbic-invalid | link-flap | loopback | pagp-flap | psecure-violation | security-violation | udld |unicast-flood | vmps} | {interval interval}

Syntax Description	cause	Enable the error-disabled mechanism to recover from a specific cause.
	all	Enable the timer to recover from all error-disabled causes.
	bpduguard	Enable the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
	channel-misconfig	Enable the timer to recover from the EtherChannel misconfiguration error-disabled state.
	dhcp-rate-limit	Enable the timer to recover from the DHCP snooping error-disabled state.
	gbic-invalid	Enable the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disable state.
		Note This error refers to an invalid small form-factor pluggable (SFP) error-disable state.
	link-flap	Enable the timer to recover from the link-flap error-disabled state.
	loopback	Enable the timer to recover from a loopback error-disabled state.
	pagp-flap	Enable the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.
	psecure-violation	Enable the timer to recover from a port security violation disable state.
	security-violation	Enable the timer to recover from an IEEE 802.1x-violation disabled state
	udld	Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
	unicast-flood	Enable the timer to recover from the unicast flood disable state.
	vmps	Enable the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state.
	interval interval	Specify the time to recover from the specified error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.
		Note The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

err-disabled

Note

Though visible in the command-line help strings, the **arp-inspection**, **storm-control**, and **unicast-flood** keywords are not supported.

Defaults	Recovery is disabled for all causes.				
	The default recover	y interval is 3	300 seconds.		
Command Modes	Global configuratio	n			
Command History	Release	Modifi	cation		
	12.2(25)EX	This co	ommand was introduced.		
Usage Guidelines	A cause (all , bpduguard and so forth) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state, an operational state similar to link-down state. If you do not enable errdisable recovery for the cause, the interface stays in error-disabled state until you enter a shutdown and no shutdown interface configuration command. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.				
	Otherwise, you mus from the error-disab		utdown then no shutdown commands to manually recover an interface		
Examples	This example shows how to enable the recovery timer for the BPDU guard error-disabled cause: Switch(config)# errdisable recovery cause bpduguard				
	This example shows how to set the timer to 500 seconds:				
	Switch(config)# errdisable recovery interval 500				
	You can verify your settings by entering the show errdisable recovery privileged EXEC command.				
Related Commands	Command		Description		
	show errdisable re	ecovery	Displays errdisable recovery timer information.		
	show interfaces sta	atus	Displays interface status or a list of interfaces in error-disabled		

state.

exceed-action

Use the **exceed-action** policy-map class police configuration command to set multiple actions for a policy-map class for packets that do not conform to the committed information rate (CIR). Use the **no** form of this command to cancel the action or return to the default action.

- exceed-action {drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit]}
- no exceed-action {drop | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit qos-group-value | transmit]}

Syntax Description	drop	Drop the packet.
	set-cos-transmit new-cos-value	Set a new class of service (CoS) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.
	set-dscp-transmit new-dscp-value	Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DCSP value is 0 to 63.
	set-prec-transmit new-precedence-value	Set a new IP precedence value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.
	set-qos-transmit qos-group-value	Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new QoS value is 0 to 99.
	cos	(Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
	dscp	(Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
	precedence	(Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.
	table table-map name	(Optional) Used in conjunction with the preceding <i>from-type</i> keyword. Specify the table map to be used for the enhanced packet marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i> parameter of the action using this table map.
	transmit	(Optional) Send the packet unmodified.

Defaults

The default action is to drop the packet.

Command Modes	ce configuration			
Command History	Release	Modification		
-	12.2(25)EX	This command was introduced.		
	12.2(25)SEG	Increased support for configuring exceed actions. See "Usage Guidelines."		
Usage Guidelines	Beginning with Cisco IOS Release 12.2(25)SEG, you can configure exceed-action to send the packet unmodified, perform marking using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. This release also added support for the ability to mark multiple QoS parameters for the same class, and configure conform-action marking and exceed-action marking simultaneously.			
	Access policy-map class police configuration mode by entering the police policy-map class command. See the police command for more information.			
	You can use this command to set one or more exceed actions for a traffic class.			
Examples	This example shows how configure multiple actions in a policy map that sets an information rate of 23000 bits per second (bps) and a burst rate of 10000 bps:			
	<pre>Switch(config)# policy-map map1 Switch(config-pmap)# class class1 Switch(config-pmap-c)# police 23000 10000 Switch(config-pmap-c-police)# conform-action transmit Switch(config-pmap-c-police)# exceed-action set-prec-transmit prec table policed-prec-table-map-name Switch(config-pmap-c-police)# 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.		
	conform-action	Defines the action to take on traffic that conforms to the CIR.		
	police	Defines a policer for classified traffic.		
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.		
	show policy-mapDisplays quality of service (QoS) policy maps.			

flowcontrol

Use the **flowcontrol** interface configuration command to set the receive flow-control state for an interface. When flow control **send** is operable and on for a device and it detects any congestion at its end, it notifies the link partner or the remote device of the congestion by sending a pause frame. When flow control **receive** is on for a device and it receives a pause frame, it stops sending any data packets. This prevents any loss of data packets during the congestion period.

Use the receive off keywords to disable flow control.

flowcontrol receive {desired | off | on}



The Cisco ME switch can only receive pause frames.

Syntax Description	receive	Set whether the interface can receive flow-control packets from a remote device.		
	desired	Allow an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.		
	off	Turn off the ability of an attached device to send flow-control packets to an interface.		
	on	Allow an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.		
Defaults	The default	is flowcontrol receive off .		
Command Modes	Interface configuration			
Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
Usage Guidelines	(UNI), you	does not support sending flow-control pause frames. If the port is a user network interface must use the no shutdown interface configuration command to enable it before using the command. UNIs are disabled by default. Network node interfaces (NNIs) are enabled by		
	Note that the on and desired keywords have the same result.			
	•	se the flowcontrol command to set a port to control traffic rates during congestion, you are control on a port to one of these conditions:		
		on or desired: The port cannot send out pause frames, but can operate with an attached that is required to or is able to send pause frames; the port is able to receive pause frames.		
	• receive given to	off: Flow control does not operate in either direction. In case of congestion, no indication is		

Table 2-2 shows the flow control results on local and remote ports for a combination of settings. The table assumes that **receive desired** has the same results as using the **receive on** keywords.

Table 2-2	Flow Control Settings and Local and Remote Port Flow Control Resolution	
-----------	---	--

Flow Control Settings		Flow Control Resolution	
Local Device	Remote Device	Local Device	Remote Device
send off/receive on	send on/receive on	Receives only	Sends and receives
	send on/receive off	Receives only	Sends only
	send desired/receive on	Receives only	Sends and receives
	send desired/receive off	Receives only	Sends only
	send off/receive on	Receives only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send off/receive off	send on/receive on	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Does not send or receive	Does not send or receive
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Does not send or receive	Does not send or receive
	send off/receive off	Does not send or receive	Does not send or receive

Examples This example shows how to configure the local port to not support flow control by the remote port:

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# flowcontrol receive off

You can verify your settings by entering the show interfaces privileged EXEC command.

Related Commands	Command Description	
	show interfaces	Displays the interface settings on the switch, including input and output flow control.

interface port-channel

Use the **interface port-channel** global configuration command to access or create the port-channel logical interface. Use the **no** form of this command to remove the port-channel.

interface port-channel port-channel-number

no interface port-channel port-channel-number

		Port-channel number. The range is 1 to 48.	
Defaults	No port-channel logical interfaces are defined.		
Command Modes	Global configuration		
Command History	Release	Modification	
-	12.2(25)EX	This command was introduced.	
Usage Guidelines	physical port to a chann command. It automatica physical port. If you cre as the <i>port-channel-num</i>	hels, you do not have to create a port-channel interface first before assigning a el group. Instead, you can use the channel-group interface configuration illy creates the port-channel interface when the channel group gets its first eate the port-channel interface first, the <i>channel-group-number</i> can be the same <i>iber</i> , or you can use a new number. If you use a new number, the channel-group creates a new port channel.	
	Only one port channel in a channel group is allowed.		
	Follow these guidelines when you use the interface port-channel command:		
		he Cisco Discovery Protocol (CDP), you must configure it only on the physical port-channel interface.	
	Note CDP is available	e only on network node interfaces (NNIs).	
	• Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.		
	For a complete list of co software configuration g	onfiguration guidelines, see the "Configuring EtherChannels" chapter in the guide for this release.	

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel** *channel-group-number* **detail** privileged EXEC command.

Related Commands	Command	Description
	channel-group	Assigns an Ethernet port to an EtherChannel group.
	show etherchannel Displays EtherChannel information for a channel.	
	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.

interface range

Use the **interface range** global configuration command to enter interface range configuration mode and to execute a command on multiple ports at the same time. Use the **no** form of this command to remove an interface range.

interface range {port-range | macro name}

no interface range {*port-range* | **macro** *name*}

Syntax Description	port-range	Port range. For a list of valid values for <i>port-range</i> , see the "Usage Guidelines" section.	
	macro name	Specify the name of a macro.	
Defaults	This command h	nas no default setting.	
Command Modes	Global configura	ation	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	When you enter all interfaces wi	interface range configuration mode, all interface parameters you enter are attributed to thin the range.	
	(SVIs). To displa displayed canno	a can use the interface range command only on existing VLAN switch virtual interfaces ay VLAN SVIs, enter the show running-config privileged EXEC command. VLANs not t be used in the interface range command. The commands entered under interface l are applied to all existing VLAN SVIs in the range.	
	All configuration changes made to an interface range are saved to NVRAM, but the interface range itself is not saved to NVRAM.		
	You can enter th	e interface range in two ways:	
	• Specifying u	up to five interface ranges	
	• Specifying a	a previously defined interface-range macro	
	All interfaces in	a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports,	

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs. However, you can define up to five interface ranges with a single command, with each range separated by a comma.

Valid values for *port-range* type and interface:

- vlan vlan-ID vlan-ID, where VLAN ID is from 1 to 4094
- **fastethernet module**/{*first port*} {*last port*}, where module is always **0**
- **gigabitethernet** *module*/{*first port*} {*last port*}, where module is always **0** For physical interfaces:

1 2

- module is always 0
- the range is type 0/number number (for example, gigabitethernet0/1 2)
- **port-channel** *port-channel-number port-channel-number*, where *port-channel-number* is from 1 to 48

Note

When you use the **interface range** command with port channels, the first and last port channel number in the range must be active port channels.

When you define a range, you must enter a space between the first entry and the hyphen (-):

```
interface range gigabitethernet0/1 -2
```

When you define multiple ranges, you must still enter a space after the first entry and before the comma (,):

```
interface range fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

You cannot specify both a macro and an interface range in the same command.

A single interface can also be specified in *port-range* (this would make the command similar to the **interface**-*id* global configuration command).

Note

For more information about configuring interface ranges, see the software configuration guide for this release.

Examples

This example shows how to use the **interface range** command to enter interface range configuration mode to apply commands to two ports:

```
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)#
```

This example shows how to use a port-range macro *macrol* for the same function. The advantage is that you can reuse *macrol* until you delete it.

```
Switch(config)# define interface-range macrol gigabitethernet0/1 - 2
Switch(config)# interface range macro macrol
Switch(config-if-range)#
```

Related Commands	Command	Description
	define interface-range	Creates an interface range 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.

interface vlan

Use the **interface vlan** global configuration command to create or access a VLAN and to enter interface configuration mode. Use the **no** form of this command to delete a VLAN.

interface vlan vlan-id

no interface vlan vlan-id

Syntax Description	vlan-id	VLAN number. The range is 1 to 4094.		
Defaults	The default VLAN interface is VLAN 1.			
Command Modes	Global configuration			
Command History	Release	Modification		
	12.2.(25)EX	This command was introduced.		
Usage Guidelines	VLANs are created the first time that you enter the interface vlan <i>vlan-id</i> command for a particular <i>vlan</i> . The <i>vlan-id</i> corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.			
•	If you delete a VLAN by entering the no interface vlan <i>vlan-id</i> command, the deleted interface is no longer visible in the output from the show interfaces privileged EXEC command.			
Note	You cannot delete the VLAN 1 interface.			
		deleted VLAN by entering the interface vlan <i>vlan-id</i> command for the deleted face comes back up, but much of the previous configuration will be gone.		
Examples	This example shows how to create a new VLAN with VLAN ID 23 and enter interface configuration mode:			
	Switch(config)# interface vlan 23 Switch(config-if)#			
	You can verify your EXEC commands.	setting by entering the show interfaces and show interfaces vlan <i>vlan-id</i> privileged		
Related Commands	Command	Description		
	show interfaces vla			

ip access-group

Use the **ip access-group** interface configuration command to control access to a Layer 2 interface. Use the **no** form of this command to remove all access groups or the specified access group from the interface.

ip access-group {*access-list-number* | *name*} {**in**}

no ip access-group [access-list-number | name] {**in**}

Syntax Description	access-list-number	The number of the IP access control list (ACL). The range is 1 to 199 or 1300 to 2699.	
	name	The name of an IP ACL, specified in the ip access-list global configuration command.	
	in	Specify filtering on inbound packets.	
Defaults	No access list is applie	ed to the interface.	
Command Modes	Interface configuration	1	
Command History	Release	Modification	
-	12.2(25)EX	This command was introduced.	
Usage Guidelines	access list by name, us list, use the access list	or numbered standard or extended IP access lists to an interface. To define an se the ip access-list global configuration command. To define a numbered access global configuration command. You can used numbered standard access lists and 1300 to 1999 or extended access lists ranging from 100 to 199 and 2000 to	
	You can use this command to apply an access list to a Layer 2 interface. However, note these limitations for port ACLs:		
	• You can only apply ACLs in the inbound direction.		
	• You can only apply one IP ACL and one MAC ACL per interface.		
	• Port ACLs do not	support logging; if the log keyword is specified in the IP ACL, it is ignored.	
		d to an interface only filters IP packets. To filter non-IP packets, use the mac rface configuration command with MAC extended ACLs.	

You can use input port ACLs and VLAN maps on the same switch. However, a port ACL takes precedence over a VLAN map. When both an input port ACL and a VLAN map are applied, incoming packets received on ports with the port ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.

For standard inbound access lists, after the switch receives a packet, it checks the source address of the packet against the access list. IP extended access lists can optionally check other fields in the packet, such as the destination IP address, protocol type, or port numbers. If the access list permits the packet, the switch continues to process the packet. If the access list denies the packet, the switch discards the packet.

If the specified access list does not exist, all packets are passed.

 Examples
 This example shows how to apply IP access list 101 to inbound packets on a port:

 Switch(config)# interface gigabitethernet0/1

 Switch(config-if)# ip access-group 101 in

You can verify your settings by entering the **show ip interface**, **show access-lists**, or **show ip access-lists** privileged EXEC command.

Related Commands	Command	Description
	access list	Configures a numbered ACL. 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 ACL. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands.
	show access-lists	Displays ACLs configured on the switch.
	show ip interface	Displays information about interface status and configuration. For syntax information, select Cisco IOS IP Command Reference , Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands .

ip address

Use the **ip address** interface configuration command to set an IP address for the Layer 2 switch. Use the **no** form of this command to remove an IP address or to disable IP processing.

ip address ip-address subnet-mask [secondary]

no ip address [*ip-address subnet-mask*] [**secondary**]

Syntax Description	ip-address	IP address.	
	subnet-mask	Mask for the associated IP subnet.	
	secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.	
Defaults	No IP address is de:	fined.	
Command Modes	Interface configurat	ion	
Command History	Release	Modification	
	12,2(25)EX	This command was introduced.	
	message. Routers respond to this request with an ICMP Mask Reply message. You can disable IP processing on a particular interface by removing its IP address with the no ip address command. If the switch detects another host using one of its IP addresses, it will send an error message to the console		
		pdates with secondary source addresses. IP broadcasts and ARP requests are handled orface routes in the IP routing table.	
Note	must also use a seco	If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.	
	remove the switch I	ves its IP address from a Bootstrap Protocol (BOOTP) or a DHCP server and you P address by using the no ip address command, IP processing is disabled, and the CP server cannot reassign the address.	

Examples This example shows how to configure the IP address for the Layer 2 switch on a subnetted network: Switch(config)# interface vlan 1 Switch(config-if)# ip address 172.20.128.2 255.255.0

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

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_comma nd_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

ip dhcp snooping

Use the **ip dhcp snooping** global configuration command to globally enable DHCP snooping. Use the **no** form of this command to return to the default setting.

ip dhcp snooping

no ip dhcp snooping

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

- **Defaults** DHCP snooping is disabled.
- Command Modes Global configuration

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

Usage GuidelinesFor any DHCP snooping configuration to take effect, you must globally enable DHCP snooping.DHCP snooping is not active until you enable snooping on a VLAN by using the **ip dhcp snooping vlan**
vlan-id global configuration command.

Examples	This example shows how to enable DHCP snooping:
	Switch(config)# ip dhcp snooping
	You can verify your settings by entering the show ip dhcp snooping privileged EXEC command.

Related Commands	Command	Description
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding information.

ip dhcp snooping binding

Use the **ip dhcp snooping binding** privileged EXEC command to configure the DHCP snooping binding database and to add binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

ip dhcp snooping binding mac-address **vlan** vlan-id ip-address **interface** interface-id **expiry** seconds

no ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id

Syntax Description	mac-address	Specify a MAC address.
	vlan vlan-id	Specify a VLAN number. The range is from 1 to 4904.
	ip-address	Specify an IP address.
	interface interface-id	Specify an interface on which to add or delete a binding entry.
	expiry seconds	Specify the interval (in seconds) after which the binding entry is no longer valid. The range is from 1 to 4294967295.
Defaults	No default database is d	lefined.
Command Modes	Privileged EXEC	
Command History	Release Modi	ification
	12.2(25)EX This	command was introduced.
Usage Guidelines	Use this command when	n you are testing or debugging the switch.
J	In the DHCP snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database can have up to 8192 bindings.	
	Use the show ip dhcp snooping binding privileged EXEC command to display only the dynamically configured bindings. Use the show ip source binding privileged EXEC command to display the dynamically and statically configured bindings.	

Examples	This example shows how to generate a DHCP binding configuration with an expiration time of 1000 seconds on a port in VLAN 1:		
	Switch# ip dhcp snooping bindin gigabitethernet0/1 expiry 1000	g 0001.1234.1234 vlan 1 172.20.50.5 interface	
	You can verify your settings by enter binding privileged EXEC comman	ring the show ip dhcp snooping binding or the show ip dhcp source d.	
Related Commands	Command	Description	
	ip dhcp snooping	Enables DHCP snooping on a VLAN.	
	show ip dhcp snooping binding	Displays the dynamically configured bindings in the DHCP snooping binding database and the configuration information.	

ip dhcp snooping database

Use the **ip dhcp snooping database** global configuration command to configure the DHCP snooping binding database agent. Use the **no** form of this command to disable the agent, to reset the timeout value, or to reset the write-delay value.

ip dhcp snooping database {{flash:/filename | ftp://user:password@host/filename |
 http://[[username:password]@]{hostname | host-ip}[/directory]/image-name.tar |
 rcp://user@host/filename | tftp://host/filename} | timeout seconds | write-delay seconds}

no ip dhcp snooping database [timeout | write-delay]

Syntax Description	flash:/filename	Specify that the database agent or the binding file is in the flash memory.	
	ftp://user:password@host/filename	Specify that the database agent or the binding file is on an FTP server.	
	http://[[username:password]@] {hostname host-ip}[/directory] /image-name.tar	Specify that the database agent or the binding file is on an FTP server.	
	rcp: //user@host/filename	Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.	
	tftp://host/filename	Specify that the database agent or the binding file is on a TFTP server.	
Defaults	timeout seconds	Specify (in seconds) when to stop the database transfer process after the DHCP snooping binding database changes.	
		The default is 300 seconds. The range is from 0 to 86400. Use 0 to define an infinite duration.	
	write-delay seconds	Specify (in seconds) the duration for which the transfer should be delayed after the binding database changes. The default is 300 seconds. The range is from 15 to 86400.	
	The URL for the database agent or binding file is not defined.		
	The timeout value is 300 seconds (5 minutes).		
	The write-delay value is 300 seconds (5 minutes).		
Command Modes	Global configuration		
Command Modes			
Command History	Release Modification		

Usage Guidelines	The DHCP snooping binding database can have up to 8192 bindings.		
	To ensure that the lease time in the database is accurate, we recommend that Network Time Protocol (NTP) is enabled and configured for these features:		
	• NTP authentication		
	• NTP peer and server associations		
	NTP broadcast service		
	NTP access restrictions		
	• NTP packet source IP address		
	If NTP is configured, the switch write clock is synchronized with NTP.	tes binding changes to the binding file only when the switch system	
	 Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store a binding file on a TFTP server. You must create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can write bindings to the binding file at that URL for the first time. Use the no ip dhcp snooping database command to disable the agent. Use the no ip dhcp snooping database timeout command to reset the timeout value. 		
	Use the no ip dhcp snooping database write-delay command to reset the write-delay value.		
Examples	This example shows how to store a binding file at an IP address of 10.1.1.1 that is in a directory called <i>directory</i> . A file named <i>file</i> must be present on the TFTP server.		
	Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file		
	You can verify your settings by entering the show ip dhcp snooping database privileged EXEC command.		
	-		
Related Commands	Command	Description	
	ip dhep snooping	Enables DHCP snooping on a VLAN.	
	ip dhcp snooping binding	Configures the DHCP snooping binding database.	
	show ip dhcp snooping database	Displays the status of DHCP snooping database agent.	

2.93

Г

ip dhcp snooping information option

Use the **ip dhcp snooping information option** global configuration command to enable DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

ip dhcp snooping information option

no ip dhcp snooping information option

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

Defaults DHCP option-82 data insertion is enabled.

Command Modes Global configuration

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

Usage Guidelines You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled and a switch receives a DHCP request from a host, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, **vlan-mod-port**, from which the packet is received (circuit ID suboption). The switch forwards the DHCP request that includes the option-82 field to the DHCP server.

When the DHCP server receives the packet, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or a circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.

The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch inspects the remote ID and possibly the circuit ID fields to verify that it originally inserted the option-82 data. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP host that sent the DHCP request.

Examples

This example shows how to enable DHCP option-82 data insertion:

Switch(config)# ip dhcp snooping information option

You can verify your settings by entering the show ip dhcp snooping privileged EXEC command.

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

ip dhcp snooping information option allowed-untrusted

Use the **ip dhcp snooping information option allowed-untrusted** global configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch. Use the **no** form of this command to configure the switch to drop these packets from the edge switch.

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Syntax Description	This command has no arguments or keywords.		
Defaults	-	DHCP packets with option-82 information that are received on untrusted ports that ed to an edge switch.	
Command Modes	Global configurat	ion	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	the edge of your n snooping, IP source aggregation switch packets with optic	n edge switch to which a host is connected to insert DHCP option-82 information at network. You might also want to enable DHCP security features, such as DHCP ce guard, or dynamic Address Resolution Protocol (ARP) inspection, on an h. However, if DHCP snooping is enabled on the aggregation switch, the switch drops on-82 information that are received on an untrusted port and does not learn DHCP s for connected devices on a trusted interface.	
	snooping on an ag command on the a though the aggreg enable DHCP seco	to which a host is connected inserts option-82 information and you want to use DHCP gregation switch, enter the ip dhcp snooping information option allowed-untrusted aggregation switch. The aggregation switch can learn the bindings for a host even gation switch receives DHCP snooping packets on an untrusted port. You can also urity features on the aggregation switch. The port on the edge switch to which the h is connected must be configured as a trusted port.	
<u>Note</u>	-	o dhcp snooping information option allowed-untrusted command on an aggregation n untrusted device is connected. If you enter this command, an untrusted device might	

spoof the option-82 information.

Examples This example shows how to configure an access switch to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

Switch(config)# ip dhcp snooping information option allowed-untrusted

You can verify your settings by entering the show ip dhcp snooping privileged EXEC command.

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

ip dhcp snooping information option format remote-id

Use the **ip dhcp snooping information option format remote-id** global configuration command to configure the option-82 remote-ID suboption. Use the **no** form of this command to configure the default remote-ID suboption.

ip dhcp snooping information option format remote-id [string ASCII-string | hostname]

no ip dhcp snooping information option format remote-id

Syntax Description	string ASCII-string	Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).
	hostname	Specify the switch hostname as the remote ID.
Defaults	The switch MAC addre	ess is the remote ID.
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(25)SEG	This command was introduced.
Usage Guidelines	command for any DHC When the option-82 fea	ble DHCP snooping by using the ip dhcp snooping global configuration CP snooping configuration to take effect. ature is enabled, the default remote-ID suboption is the switch MAC address. This
	command allows you t (but no spaces) to be th	to configure either the switch hostname or a string of up to 63 ASCII characters he remote ID.
Note	If the hostname exceed	ds 63 characters, it is truncated to 63 characters in the remote-ID configuration.
Examples	Switch(config)# ip c	ow to configure the option-82 remote-ID suboption: The psnooping information option format remote-id hostname
	You can verify your se	ettings by entering the show ip dhcp snooping user EXEC command.
Related Commands	Command	Description
	ip dhcp snooping vla option format-type ci	
	show ip dhcp snoopin	ng Displays the DHCP snooping configuration.

ip dhcp snooping limit rate

Use the **ip dhcp snooping limit rate** interface configuration command to configure the number of DHCP messages an interface can receive per second. Use the **no** form of this command to return to the default setting.

ip dhcp snooping limit rate rate

no ip dhcp snooping limit rate

Syntax Description	rate	Number of DHCP messages an interface can receive per second. The range is 1 to 2048.
Defaults	DHCP snooping	ate limiting is disabled.
Command Modes	Interface configu	ation
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	interfaces, keep i	e limit applies to untrusted interfaces. If you want to configure rate limiting for trusted a mind that trusted interfaces might aggregate DHCP traffic on multiple VLANs (some of be snooped) in the switch, and you will need to adjust the interface rate limits to a
	errdisable recover again when all the transformer of the second s	exceeded, the interface is error-disabled. If you enabled error recovery by entering the ery dhcp-rate-limit global configuration command, the interface retries the operation e causes have timed out. If the error-recovery mechanism is not enabled, the interface disabled state until you enter the shutdown and no shutdown interface configuration
Examples	-	ws how to set a message rate limit of 150 messages per second on an interface: E(t) # ip dhep snooping limit rate 150
		ur settings by entering the show ip dhcp snooping privileged EXEC command.
Related Commands	Command	Description
	errdisable reco	ery Configures the recover mechanism.
	show ip dhcp si	ooping Displays the DHCP snooping configuration.

Displays the DHCP snooping binding information.

show ip dhcp snooping binding

ip dhcp snooping trust

Use the **ip dhcp snooping trust** interface configuration command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to return to the default setting.

ip dhcp snooping trust

no ip dhcp snooping trust

Syntax Description	This command has no arguments or keywords.		
Defaults	DHCP snooping trus	t is disabled.	
Command Modes	Interface configuration	on	
Command History	Release	Modification	
2	12.2(25)EX	This command	l was introduced.
Usage Guidelines	-		are connected to a DHCP server or to other switches or routers. at are connected to DHCP clients.
Examples	This example shows	how to enable D	HCP snooping trust on a port:
	Switch(config-if)# ip dhcp snooping trust		
	You can verify your s	settings by enter	ing the show ip dhcp snooping privileged EXEC command.
Related Commands	Command		Description
	show ip dhcp snoop	ing	Displays the DHCP snooping configuration.
	show ip dhcp snoop	oing binding	Displays the DHCP snooping binding information.

ip dhcp snooping verify mac-address

Use the **ip dhcp snooping verify mac-address** global configuration command to configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to configure the switch to not verify the MAC addresses.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Syntax Description	This command has no arguments or keywords.

Defaults The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

Command Modes Global configuration

 Release
 Modification

 12.2(25)EX
 This command was introduced.

Usage Guidelines In a service-provider network, when a switch receives a packet from a DHCP client on an untrusted port, it automatically verifies that the source MAC address and the DHCP client hardware address match. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

Examples This example shows how to disable the MAC address verification:

Switch(config) # no ip dhcp snooping verify mac-address

You can verify your settings by entering the show ip dhcp snooping privileged EXEC command.

Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP snooping configuration.

ip dhcp snooping vlan

Use the **ip dhcp snooping vlan** global configuration command to enable DHCP snooping on a VLAN. Use the **no** form of this command to disable DHCP snooping on a VLAN.

ip dhcp snooping vlan vlan-range

no ip dhcp snooping vlan vlan-range

Syntax Description	vlan vlan-range	Specify a VLAN range is 1 to 409	ID or a range of VLANs on which to enable DHCP snooping. The 4.
		IDs separated by	ingle VLAN ID identified by VLAN ID number, a series of VLAN commas, a range of VLAN IDs separated by hyphens, or a range parated by entering the starting and ending VLAN IDs separated
Defaults	DHCP snooping is	s disabled on all V	LANs.
Command Modes	Global configurat	on	
Command History	Release	Modification	
	12.2(25)EX	This command	d was introduced.
Usage Guidelines	You must first glo	bally enable DHC	P snooping before enabling DHCP snooping on a VLAN.
Examples	This example show	ws how to enable I	DHCP snooping on VLAN 10:
	Switch(config)#	ip dhcp snooping	y vlan 10
	You can verify yo	ur settings by ente	ring the show ip dhcp snooping privileged EXEC command.
Related Commands	Command		Description
	show ip dhcp sno	ooping	Displays the DHCP snooping configuration.
	show ip dhcp sno	oping binding	Displays the DHCP snooping binding information.

ip dhcp snooping vlan information option format-type circuit-id string

Use the **ip dhcp snooping vlan information option format-type circuit-id string** interface configuration command to configure the option-82 circuit-ID suboption. Use the **no** form of this command to configure the default circuit-ID suboption.

ip dhcp snooping vlan vlan-id information option format-type circuit-id string ASCII-string

no ip dhcp snooping vlan vlan-id information option format-type circuit-id string

Syntax Description	vlan vlan-id	Specify the VLAN ID. The range is 1 to 4094.	
	string ASCII-strin	g Specify a circuit ID, using from 3 to 63 ASCII characters (no spaces).	
Defaults	The switch VLAN	and the port identifier, in the format vlan-mod-port , is the default circuit ID.	
Command Modes	Interface configur	tion	
Command History	Release	Modification	
	12.2(25)SEG	This command was introduced.	
Usage Guidelines	You must globally enable DHCP snooping by using the ip dhcp snooping global configuration command for any DHCP snooping configuration to take effect.		
•	When the option-82 feature is enabled, the default circuit-ID suboption is the switch VLAN and the port identifier, in the format vlan-mod-port . This command allows you to configure a string of ASCII characters to be the circuit ID.		
Note	When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.		
Examples	This example show	vs how to configure the option-82 circuit-ID suboption:	
	Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id string customerABC-250-0-0		
	You can verify you	r settings by entering the show ip dhcp snooping user EXEC command.	



The **show ip dhcp snooping** user EXEC command only displays the global command output, including a remote-ID configuration. It does not display any per-interface, per-VLAN string that you have configured for the circuit ID.

Related Commands

Command	Description
ip dhcp snooping information option format remote-id	Configures the option-82 remote-ID suboption.
show ip dhcp snooping	Displays the DHCP snooping configuration.

ip igmp filter

Use the **ip igmp filter** interface configuration command to control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface. Use the **no** form of this command to remove the specified profile from the interface.

ip igmp filter *profile number*

no ip igmp filter

Syntax Description	profile number	The IGMP profile number to be applied. The range is 1 to 4294967295.	
Defaults	No IGMP filters a	re applied.	
Command Modes	Interface configur	ation	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to ports that belong to an EtherChannel group. An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.		
Examples	Switch(config)#	ws how to apply IGMP profile 22 to a port. interface gigabitethernet0/2) # ip igmp filter 22	
	You can verify yo specifying an inte	ur setting by using the show running-config privileged EXEC command and by rface.	
Related Commands	Command	Description	
	ip igmp profile	Configures the specified IGMP profile number.	

Command	Description
show ip dhcp snooping statistics	Displays the characteristics of the specified IGMP profile.
show running-config interface <i>interface-id</i>	Displays the running configuration on the switch interface, including the IGMP profile (if any) that is applied to an interface. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands .

ip igmp max-groups

Use the **ip igmp max-groups** interface configuration command to set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table. Use the **no** form of this command to set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report.

ip igmp max-groups {*number* | **action** {**deny** | **replace**}}

no ip igmp max-groups {*number* | **action**}

Syntax Description	number	The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit.		
	action deny	When the maximum number of entries is in the IGMP snooping forwarding table, drop the next IGMP join report. This is the default action.		
	action replace	When the maximum number of entries is in the IGMP snooping forwarding table, replace the existing group with the new group for which the ICMP report was received.		
Defaults	The default m	aximum number of groups is no limit.		
	throttling action	ch learns the maximum number of IGMP group entries on an interface, the default on is to drop the next IGMP report that the interface receives and to not add an entry for up to the interface.		
Command Modes	Interface conf	iguration		
Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
Usage Guidelines	You can use the	his command only on Layer 2 physical interfaces and on logical EtherChannel interfaces.		
	You cannot set IGMP maximum groups for ports that belong to an EtherChannel group.			
	Follow these guidelines when configuring the IGMP throttling action:			
	• If you configure the throttling action as deny and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.			
	that were	figure the throttling action as replace and set the maximum group limitation, the entries previously in the forwarding table are removed. When the maximum number of entries is warding table, the switch replaces a randomly-selected multicast entry with the received ort.		
		maximum group limitation is set to the default (no maximum), entering the ip igmp ips { deny replace } command has no effect.		

Examples This example shows how to limit to 25 the number of IGMP groups that a port can join. Switch(config)# interface gigabitethernet0/2 Switch(config-if)# ip igmp max-groups 25

This example shows how to configure the switch to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp max-groups action replace

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

Related Commands	Command	Description
	8 8	Displays the running configuration on the switch interface, including
	interface-id	the maximum number of IGMP groups that an interface can join and
		the throttling action. For syntax information, select Cisco IOS
		Configuration Fundamentals Command Reference, Release 12.2 >
		File Management Commands > Configuration File Management
		Commands.

ip igmp profile

Use the **ip igmp profile** global configuration command to create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switchport. Use the **no** form of this command to delete the IGMP profile.

ip igmp profile *profile number*

no ip igmp profile profile number

Curtos Deceription				
Syntax Description	profile number	The IGMP profile number being configured. The range is 1 to 4294967295.		
Defaults	deny matching addresses.			
Command Modes				
Command History	Release	Modification		
	12.2.(25)EX	This command was introduced.		
Usage Guidelines	When you are in IGMP profile configuration mode, you can create the profile by using these commands:			
	• deny : specifies that matching addresses are denied; this is the default condition.			
	• exit: exits from igmp-profile configuration mode.			
	 no: negates a command or resets to its defaults. permit: specifies that matching addresses are permitted. range: specifies a range of IP addresses for the profile. This can be a single IP address or a rang with a start and an end address. 			
	When entering a range, enter the low IP multicast address, a space, and the high IP multicast addre			
	You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only or profile applied to it.			
Examples	This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses.			
	Switch(config)# ip igmp profile 40 Switch(config-igmp-profile)# permit Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255			
	You can verify yo	ur settings by using the show ip igmp profile privileged EXEC command.		

Related Commands	Command	Description
	ip igmp filter	Applies the IGMP profile to the specified interface.
	show ip dhcp snooping statistics	Displays the characteristics of all IGMP profiles or the specified IGMP profile number.

ip igmp snooping

Use the **ip igmp snooping** global configuration command to globally enable Internet Group Management Protocol (IGMP) snooping on the switch or to enable it on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description	vlan vlan-id	(Optional) Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.	
Defaults	IGMP snooping is g	globally enabled on the switch.	
	IGMP snooping is a	enabled on VLAN interfaces.	
Command Modes	Global configuratio	n	
Command History	Release	Modification	
,	12.2(25)EX	This command was introduced.	
Usage Guidelines	When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces. When IGMP snooping is disabled globally, it is disabled on all the existing VLAN interfaces.		
	VLAN IDs 1002 to snooping.	1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP	
Examples	This example show	s how to globally enable IGMP snooping:	
	Switch(config)# ip igmp snooping		
	This example shows how to enable IGMP snooping on VLAN 1:		
	Switch(config)# ip igmp snooping vlan 1		
	You can verify your	r settings by entering the show ip igmp snooping privileged EXEC command.	

Related Commands	Command	Description
	ip igmp snooping report-suppression	Enables IGMP report suppression.
	show ip igmp snooping	Displays the snooping configuration.
	show ip igmp snooping groups	Displays IGMP snooping multicast information.
	show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
	show ip igmp snooping querier detail	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip igmp snooping last-member-query-interval

Use the **ip igmp snooping last-member-query-interval** global configuration command to enable the Internet Group Management Protocol (IGMP) configurable-leave timer globally or on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

ip igmp snooping [vlan vlan-id] last-member-query-interval time

no ip igmp snooping [vlan vlan-id] last-member-query-interval

Syntax Descriptiont	vlan vlan-id	(Optional) Enable IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.	
	time	Interval time out in seconds. The range is 100 to 5000 milliseconds.	
Defaults	The default timeout setting is 1000 milliseconds.		
Command Modes	Global configuration	on	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	1	ing is globally enabled, IGMP snooping is enabled on all the existing VLAN GMP snooping is globally disabled, IGMP snooping is disabled on all the existing	
	VLAN IDs 1002 to snooping.	1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP	
	Configuring the lea	we timer on a VLAN overrides the global setting.	
	The IGMP configu	rable leave time is only supported on devices running IGMP Version 2.	
	The configuration i	s saved in NVRAM.	
Examples	This example show	s how to globally enable the IGMP leave timer for 2000 milliseconds:	
	<pre>Switch(config)# ip igmp snooping last-member-query-interval 2000</pre>		
	This example show	s how to configure the IGMP leave timer for 3000 milliseconds on VLAN 1:	
	1		
	-	p igmp snooping vlan 1 last-member-query-interval 3000	

Related Commands 0

Command	Description	
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.	
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.	
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.	
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.	
show ip igmp snooping	Displays the IGMP snooping configuration.	

ip igmp snooping querier

Use the **ip igmp snooping querier** global configuration command to globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. Use the **no** form of this command to return to the default settings.

- **ip igmp snooping querier** [**vlan** *vlan-id*] [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** [**count** *count* | **interval** *interval*] | **timer expiry** | **version** *version*]
- **no ip igmp snooping querier [vlan** *vlan-id*] [address | max-response-time | query-interval | tcn query { count count | interval interval} | timer expiry | version]

Syntax Description	vlan vlan-id	(Optional) Enable IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
	address ip-address	(Optional) Specify a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
	max-response-time response-time	(Optional) Set the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
	query-interval <i>interval-count</i>	(Optional) Set the interval between IGMP queriers. The range is 1 to 18000 seconds.
	tcn query [count <i>count</i> / interval <i>interval</i>]	(Optional) Set parameters related to Topology Change Notifications (TCNs). The keywords have these meanings:
		• count —Set the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.
		• interval <i>interval</i> —Set the TCN query interval time. The range is 1 to 255.
	timer expiry	(Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
	version version	(Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2.
Defaults	The IGMP snooping que	erier feature is globally disabled on the switch.
		P snooping querier disables itself if it detects IGMP traffic from a
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a <i>querier</i> .
By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2) but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the max-response-time value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured and is set to zero).
Non-RFC compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the max-response-time value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.
VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.
This example shows how to globally enable the IGMP snooping querier feature:
Switch(config)# ip igmp snooping querier
This example shows how to set the IGMP snooping querier maximum response time to 25 seconds: Switch(config)# ip igmp snooping querier max-response-time 25
This example shows how to set the IGMP snooping querier interval time to 60 seconds: Switch(config)# ip igmp snooping querier query-interval 60
This example shows how to set the IGMP snooping querier TCN query count to 25: Switch(config) # ip igmp snooping querier tcn count 25
This example shows how to set the IGMP snooping querier timeout to 60 seconds: Switch(config)# ip igmp snooping querier timeout expiry 60
This example shows how to set the IGMP snooping querier feature to version 2:
Switch(config)# ip igmp snooping querier version 2
You can verify your settings by entering the show ip igmp snooping privileged EXEC command.
Command Description

Related Commands	Command	Description
	ip igmp snooping report-suppression	Enables IGMP report suppression.
	show ip igmp snooping	Displays the IGMP snooping configuration.
	show ip igmp snooping groups	Displays IGMP snooping multicast information.
	show ip igmp snooping mrouter	Displays the IGMP snooping router ports.

ip igmp snooping report-suppression

Use the **ip igmp snooping report-suppression** global configuration command to enable Internet Group Management Protocol (IGMP) report suppression. Use the **no** form of this command to disable IGMP report suppression and to forward all IGMP reports to multicast routers.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

- Syntax Description This command has no arguments or keywords.
- **Defaults** IGMP report suppression is enabled.
- Command Modes Global configuration

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

Usage Guidelines IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all the multicast routers.

ExamplesThis example shows how to disable report suppression:
Switch(config)# no ip igmp snooping report-suppression

You can verify your settings by entering the show ip igmp snooping privileged EXEC command.

Related Commands	Command	Description
	ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
	show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping tcn

Use the **ip igmp snooping tcn** global configuration command to configure the Internet Group Management Protocol (IGMP) Topology Change Notification (TCN) behavior. Use the **no** form of this command to return to the default settings.

ip igmp snooping tcn {flood query count count | query solicit}

no ip igmp snooping tcn {flood query count | query solicit}

Syntax Description	flood query count count	Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10.
	query solicit	Send an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event.
Defaults	The TCN flood query cou	nt is 2.
	The TCN query solicitatio	n is disabled.
Command Modes	Global configuration	
Command History	Release	Modification
2	12.2(25)EX	This command was introduced.
	count command, the flood flooding of multicast traffi	Te TCN flood query count to 1 by using the ip igmp snooping ten flood query ling stops after receiving one general query. If you set the count to 7, the c due to the TCN event lasts until seven general queries are received. Groups general queries received during the TCN event.
Examples	This example shows how t traffic is flooded:	o specify 7 as the number of IGMP general queries for which the multicast
	Switch(config)# no ip igmp snooping tcn flood query count 7	
	You can verify your setting	gs by entering the show ip igmp snooping privileged EXEC command.
Related Commands	Command	Description
	ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
	ip igmp snooping ten floo	
	show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping tcn flood

Use the **ip igmp snooping tcn flood** interface configuration command to specify multicast flooding as the Internet Group Management Protocol (IGMP) snooping spanning-tree Topology Change Notification (TCN) behavior. Use the **no** form of this command to disable the multicast flooding.

ip igmp snooping tcn flood

no ip igmp snooping tcn flood

Defaults Multicast flooding is enabled on an interface during a spanning-tree TCN event.

Command Modes Interface configuration

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

Usage Guidelines When the switch receives a TCN, multicast traffic is flooded to all the ports until two general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding behavior might not be desirable because the flooded traffic might exceed the capacity of the link and cause packet loss.

You can change the flooding query count by using the **ip igmp snooping tcn flood query count** global configuration command.

Examples This example shows how to disable the multicast flooding on an interface:

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no ip igmp snooping tcn flood

You can verify your settings by entering the show ip igmp snooping privileged EXEC command.

Related Commands Command Description		Description
	ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
	ip igmp snooping tcn	Configures the IGMP TCN behavior on the switch.
	show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping vlan immediate-leave

Use the **ip igmp snooping vlan** *vlan-id* **immediate-leave** global configuration command to enable Internet Group Management Protocol (IGMP) snooping immediate-leave processing on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

ip igmp snooping vlan vlan-id immediate-leave

no ip igmp snooping vlan vlan-id immediate-leave

Syntax Description		Enable IGMP snooping and the Immediate-Leave feature on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
Defaults	IGMP immediate-leave pr	ocessing is disabled.
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	VLAN IDs 1002 to 1005 a snooping.	are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP
		the Immediate Leave feature when there is a maximum of one receiver on The configuration is saved in NVRAM.
	The Immediate Leave feat	ure is supported only with IGMP Version 2 hosts.
Examples	-	to enable IGMP immediate-leave processing on VLAN 1:
		snooping vlan 1 immediate-leave gs by entering the show ip igmp snooping privileged EXEC command.
Related Commands	Command	Description
	ip igmp snooping report	-suppression Enables IGMP report suppression.
	show ip igmp snooping	Displays the snooping configuration.
	show ip igmp snooping g	groups Displays IGMP snooping multicast information.
	show ip igmp snooping i	nrouter Displays the IGMP snooping router ports.
	show ip igmp snooping o	uerier detail Displays the configuration and operation information for the IGMP querier configured on a switch.

ip igmp snooping vlan mrouter

Use the **ip igmp snooping vlan** *vlan-id* **mrouter** global configuration command to add a multicast router port or to configure the multicast learning method. Use the **no** form of this command to return to the default settings.

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

Syntax Description			
Syntax Description	vlan-id	Enable IGMP snooping, and add the port in the specified VLAN as the multicast router port. The range is 1 to 1001 and 1006 to 4094.	
	interface interface-id	Specify the next-hop interface to the multicast router. Valid interfaces are physical interfaces and port channels. The port-channel range is 1 to 48.	
	learn pim-dvmrp	Specify the multicast router learning method. The only learning method supported on the Cisco ME switch is pim-dvmrp , which sets the switch to learn multicast router ports by snooping on IGMP queries and Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets.	
Defaults	By default, there are no	multicast router ports.	
	The default learning method is pim-dvmrp —to snoop IGMP queries and PIM-DVMRP packets.		
Command Modes			
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
		This command was infoddeed.	
Usage Guidelines	VLAN IDs 1002 to 100 snooping.	5 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP	
Usage Guidelines		5 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP	
Ĵ	snooping. The configuration is sav	5 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP	
Usage Guidelines Examples	snooping. The configuration is sav This example shows how	5 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP red in NVRAM.	

ited Commands	Command	Description
	ip igmp snooping report-suppression	Enables IGMP report suppression.
	show ip igmp snooping	Displays the snooping configuration.
	show ip igmp snooping groups	Displays IGMP snooping multicast information.
	show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
	show ip igmp snooping querier detail	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip igmp snooping vlan static

Use the **ip igmp snooping vlan** *vlan-id* **static** global configuration command to enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group. Use the **no** form of this command to remove ports specified as members of a static multicast group.

ip igmp snooping vlan vlan-id static ip-address interface interface-id

no ip igmp snooping vlan vlan-id static ip-address interface interface-id

Syntax Description	vlan-id	Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
	ip-address	Add a Layer 2 port as a member of a multicast group with the specified group IP address.
	interface interface-id	Specify the interface of the member port. The keywords have these meanings:
		• fastethernet <i>interface number</i> —a Fast Ethernet IEEE 802.3 interface.
		• gigabitethernet <i>interface number</i> —a Gigabit Ethernet IEEE 802.3z interface.
		• port-channel <i>interface number</i> —a channel interface. The range is 0 to 48.
Command Modes	Global configuration	
	Global configuration	Modification
Command Modes		Modification This command was introduced.
	Release 12.2(25)EX	
Command History	Release 12.2(25)EX VLAN IDs 1002 to 100	This command was introduced. 5 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP
Command History Usage Guidelines	Release 12.2(25)EX VLAN IDs 1002 to 100 snooping. The configuration is say	This command was introduced. 5 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP
Command History	Release12.2(25)EXVLAN IDs 1002 to 100snooping.The configuration is sawThis example shows how	This command was introduced. 5 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP ved in NVRAM.

Related Commanus	ļ	Related	Commands	-	С
------------------	---	---------	----------	---	---

ated Commands	Command	Description
	ip igmp snooping report-suppression	Enables IGMP report suppression.
	show ip igmp snooping	Displays the snooping configuration.
	show ip igmp snooping groups	Displays IGMP snooping multicast information.
	show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
	show ip igmp snooping querier detail	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip ssh

Use the ip ssh global configuration command to configure the switch to run Secure Shell (SSH) Version 1 or SSH Version 2. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to return to the default setting. ip ssh version [1 | 2] no ip ssh version [1 | 2] Syntax Description 1 (Optional) Configure the switch to run SSH Version 1 (SSHv1). 2 (Optional) Configure the switch to run SSH Version 2 (SSHv1). Defaults The default version is the latest SSH version supported by the SSH client. Command Modes Global configuration **Command History** Release Modification 12.2(25)EX This command was introduced. **Usage Guidelines** If you do not enter this command or if you do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2. The switch supports an SSHv1 or an SSHv2 server. It also supports an SSHv1 client. For more information about the SSH server and the SSH client, see the software configuration guide for this release. A Rivest, Shamir, and Adelman (RSA) key pair generated by an SSHv1 server can be used by an SSHv2 server and the reverse. Examples This example shows how to configure the switch to run SSH Version 2: Switch(config) # ip ssh version 2 You can verify your settings by entering the show ip ssh or show ssh privileged EXEC command.

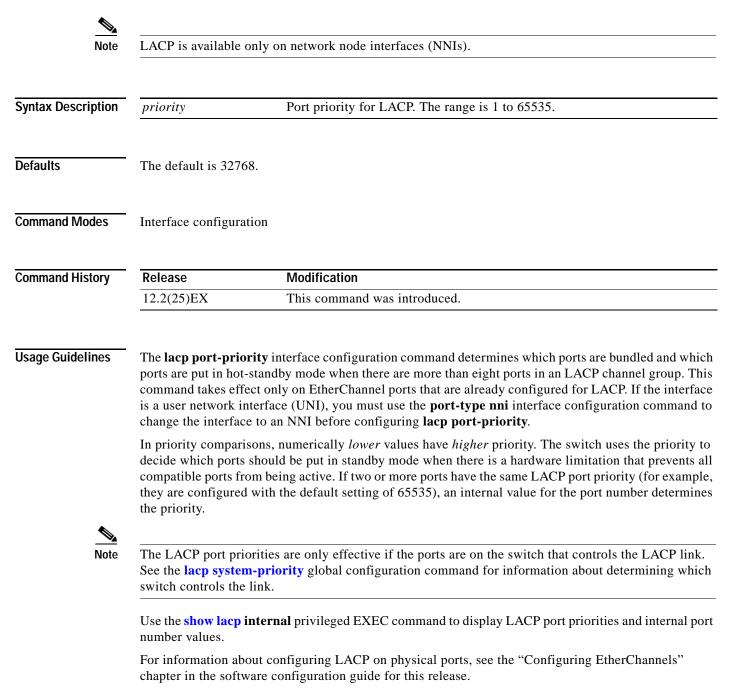
Related Commands	Command	Description
	show ip ssh	Displays if the SSH server is enabled and displays the version and configuration information for the SSH server. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features > Secure Shell Commands .
	show ssh	Displays the status of the SSH server. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features > Secure Shell Commands .

lacp port-priority

Use the **lacp port-priority** interface configuration command to configure the port priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

lacp port-priority priority

no lacp port-priority



Γ

ExamplesThis example shows how to configure the LACP port priority on a port:
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lacp port-priority 1000

You can verify your settings by entering the **show lacp** [*channel-group-number*] **internal** privileged EXEC command.

Related Commands Command

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
lacp system-priority	Configures the LACP system priority.
<pre>show lacp [channel-group-number] internal</pre>	Displays internal information for all channel groups or for the specified channel group.

lacp system-priority

Use the **lacp system-priority** global configuration command to configure the system priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

lacp system-priority priority

no lacp system-priority

Note LACP is available only on network node interfaces (NNIs). Syntax Description priority System priority for LACP. The range is 1 to 65535. Defaults The default is 32768. Command Modes Global configuration **Command History** Release Modification 12.2(25)EX This command was introduced. **Usage Guidelines** The **lacp system-priority** command determines which switch in an LACP link controls port priorities. Although this is a global configuration command, the priority only takes effect on EtherChannels that have physical ports that are already configured for LACP. An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the noncontrolling end of the link) are ignored. In priority comparisons, numerically lower values have higher priority. Therefore, the switch with the numerically lower system value (higher priority value) for LACP system priority becomes the controlling switch. If both switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control. The **lacp system-priority** command applies to all LACP EtherChannels on the switch. Use the show etherchannel summary privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag). For more information about configuring LACP on physical ports, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

ExamplesThis example shows how to set the LACP system priority:
Switch(config)# lacp system-priority 20000

You can verify your settings by entering the show lacp sys-id privileged EXEC command.

Related Commands Command De		Description
	channel-group	Assigns an Ethernet port to an EtherChannel group.
	lacp port-priority	Configures the LACP port priority.
	show lacp sys-id	Displays the system identifier that is being used by LACP.

2-131

OL-9643-02

logging event

Use the **logging event** interface configuration command to enable notification of interface link status changes. Use the **no** form of this command to disable notification.

logging event {bundle-status | link-status | spanning-tree | status | trunk status}

no logging event {bundle-status | link-status | spanning-tree | status | trunk status}

Syntax Description	bundle-status	Enable notification of BUNDLE and UNBUNDLE messages.
	link-status	Enable notification of interface data link status changes.
	spanning-tree	Enable notification of spanning-tree events.
	status	Enable notification of spanning-tree state change messages.
	trunk-status	Enable notification of trunk-status messages.
Defaults	Event logging is o	lisabled.
Command Modes	Interface configur	ration
Command History	Release	Modification
	12.2(25)SEG	This command was introduced.
Examples	-	ws how to enable spanning-tree logging: f)# logging event spanning-tree

logging file

Use the **logging file** global configuration command to set logging file parameters. Use the **no** form of this command to return to the default setting.

logging file filesystem: filename [max-file-size [min-file-size]] [severity-level-number | type]

no logging file *filesystem:filename* [*severity-level-number* | *type*]

Syntax Description	filesystem:filename	Alias for a flash file system. Contains the path and name of the file that contains the log messages.
		The syntax for the local flash file system: flash:
	max-file-size	(Optional) Specify the maximum logging file size. The range is 4096 to 2147483647.
	min-file-size	(Optional) Specify the minimum logging file size. The range is 1024 to 2147483647.
	severity-level-number	(Optional) Specify the logging severity level. The range is 0 to 7. See the <i>type</i> option for the meaning of each level.
	type	(Optional) Specify the logging type. These keywords are valid:
		• emergencies—System is unusable (severity 0).
		• alerts —Immediate action needed (severity 1).
		• critical —Critical conditions (severity 2).
		• errors —Error conditions (severity 3).
		• warnings—Warning conditions (severity 4).
		• notifications—Normal but significant messages (severity 5).
		• information —Information messages (severity 6).
		• debugging —Debugging messages (severity 7).
Defaults	The minimum file size i	as 2048 bytes; the maximum file size is 4096 bytes.
	The default severity leve	el is 7 (debugging messages and numerically lower levels).
Command Modes	Global configuration	
Command History	Release	Modification
· · · · · · · · · · · · · · · · · · ·	12.2(25)EX	This command was introduced.

	snow running-comig	link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_comma nd_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.
Related Commands	Command show running-config	Description Displays the operating configuration. For syntax information, use this
Examples	Switch(config)# logging You can verify your settin	to save informational log messages to a file in flash memory: g file flash:logfile informational ng by entering the show running-config privileged EXEC command.
	Specifying a <i>level</i> causes	messages at that level and numerically lower levels to be displayed.
	0	minimum file size if it is greater than the maximum file size minus 1024; the ecomes the maximum file size minus 1024.
	• •	sh memory by using the logging file flash: <i>filename</i> global configuration e more flash: <i>filename</i> privileged EXEC command to display its contents.
Usage Guidelines	system messages by using configured syslog server.	SCII text format in an internal buffer on the switch. You can access logged g the switch command-line interface (CLI) or by saving them to a properly If the switch fails, the log is lost unless you had previously saved it to flash ging file flash: <i>filename</i> global configuration command.

mac access-group

Use the **mac access-group** interface configuration command to apply a MAC access control list (ACL) to a Layer 2 interface. Use the **no** form of this command to remove all MAC ACLs or the specified MAC ACL from the interface. You create the MAC ACL by using the **mac access-list extended** global configuration command.

mac access-group {*name*} **in**

no mac access-group {*name*}

Syntax Description	name	Specify a named MAC access list.	
	in	Specify that the ACL is applied in the ingress direction. Outbound ACLs are not	
		supported on Layer 2 interfaces.	
Defaults	No MAC ACL	is applied to the interface.	
Command Modes	Interface conf	iguration (Layer 2 interfaces only)	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	On Layer 2 in access lists. Ye IP ACL and a	MAC ACLs only to ingress Layer 2 interfaces. terfaces, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC ou can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an MAC ACL to the interface. You can apply no more than one IP access list and one MAC he same Layer 2 interface.	
	If a MAC ACL is already configured on a Layer 2 interface and you apply a new MAC ACL to the interface, the new ACL replaces the previously configured one.		
		n ACL to a Layer 2 interface on a switch, and the switch has a VLAN map applied to a e interface is a member of, the ACL applied to the Layer 2 interface takes precedence.	
		und packet is received on an interface with a MAC ACL applied, the switch checks the ons in the ACL. If the conditions are matched, the switch forwards or drops the packet, he ACL.	
•	If the specified	d ACL does not exist, the switch forwards all packets.	
Note		rmation about configuring MAC extended ACLs, see the "Configuring Network Security hapter in the software configuration guide for this release.	

Examples This example shows how to apply a MAC extended ACL named *macacl2* to an interface:

Switch(config)# interface gigabitethernet0/1 Switch(config-if)# mac access-group macacl2 in

You can verify your settings by entering the **show mac access-group** privileged EXEC command. You can see configured ACLs on the switch by entering the **show access-lists** privileged EXEC command.

Related Commands	Command	Description
	show access-lists	Displays the ACLs configured on the switch.
	show mac access-group	Displays the MAC ACLs configured on the switch.
	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_com mand_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

mac access-list extended

Use the **mac access-list extended** global configuration command to create an access list based on MAC addresses for non-IP traffic. Using this command puts you in the extended MAC access-list configuration mode. Use the **no** form of this command to return to the default setting.

mac access-list extended name

no mac access-list extended name

Syntax Description	name Assign a name to the MAC extended access list.		
Defaults	By default, there are no MAC access lists created.		
Command Modes	Global configuration		
Command History	Release Modification		
	12.2(25)EX This command was introduced.		
	Entering the mac access-list extended command enables the MAC access-list configuration mode. These configuration commands are available:		
	• default : sets a command to its default.		
	• deny : specifies packets to reject. For more information, see the deny (MAC access-list configuration) MAC access-list configuration command.		
	• exit : exits from MAC access-list configuration mode.		
	• no : negates a command or sets its defaults.		
	• permit : specifies packets to forward. For more information, see the permit (MAC acce configuration) command.	ess-list	
•			

release.

 Examples
 This example shows how to create a MAC named extended access list named mac1 and to enter extended MAC access-list configuration mode:

Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)#

This example shows how to delete MAC named extended access list mac1:

Switch(config) # no mac access-list extended mac1

You can verify your settings by entering the show access-lists privileged EXEC command.

Related Commands	Command	Description
	deny (MAC access-list configuration)	Configures the MAC ACL (in extended MAC-access list configuration mode).
	permit (MAC access-list configuration)	
	show access-lists	Displays the access lists configured on the switch.
	vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.

mac address-table aging-time

Use the **mac address-table aging-time** global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the **no** form of this command to return to the default setting. The aging time applies to all VLANs or a specified VLAN.

mac address-table aging-time {**0** | *10-1000000*} [**vlan** *vlan-id*]

no mac address-table aging-time {**0** | *10-1000000*} [**vlan** *vlan-id*]

Syntax DescriptionI	0	This value disable the table.	s aging. Static address entries are never aged or removed from	
	10-1000000	Aging time in seco	onds. The range is 10 to 1000000 seconds.	
	vlan vlan-id	(Optional) Specify 1 to 4094.	the VLAN ID to which to apply the aging time. The range is	
Defaults	The default is 300	seconds.		
Command Modes	Global configurat	ion		
Command History	Release	Modification		
	12.2(25)EX	This comman	d was introduced.	
Usage Guidelines			se the aging time to record the dynamic entries for a longer time. bility of flooding when the hosts send again.	
	If you do not spec	ify a specific VLAN,	this command sets the aging time for all VLANs.	
Examples	This example show	ws how to set the agin	g time to 200 seconds for all VLANs:	
	<pre>Switch(config)# mac address-table aging-time 200</pre>			
	You can verify yo command.	ur setting by entering	the show mac address-table aging-time privileged EXEC	
Related Commands	Command		Description	
	show mac addre	ss-table aging-time	Displays the MAC address table aging time for all VLANs or the specified VLAN.	

2-139

mac address-table notification

Use the **mac address-table notification** global configuration command to enable the MAC address notification feature on the switch. Use the **no** form of this command to return to the default setting.

mac address-table notification [**history-size** *value*] | [**interval** *value*]

no mac address-table notification [history-size | interval]

Syntax Description	history-size value	(Optional) Configure the maximum number of entries in the MAC notification history table. The range is 1 to 500 entries.	
	interval value	(Optional) Set the notification trap interval. The switch sends the notification traps when this amount of time has elapsed. The range is 0 to 2147483647 seconds.	
Defaults	By default, the MAC a	address notification feature is disabled.	
	The default trap interv	al value is 1 second.	
	The default number of	entries in the history table is 1.	
Command Modes	Global configuration		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	address notification fe management system (I	address is added or an old address is deleted from the forwarding tables, the MAC ature sends Simple Network Management Protocol (SNMP) traps to a network NMS). MAC notifications are generated only for dynamic and secure MAC not generated for self addresses, multicast addresses, or other static addresses.	
	When you configure the history-size option, the existing MAC address history table is deleted, and a new table is created.		
	command. You must al mac-notification inter	address notification feature by using the mac address-table notification lso enable MAC address notification traps on an interface by using the snmp trap face configuration command and configure the switch to send MAC address traps he snmp-server enable traps mac-notification global configuration command.	
Examples	_	ow to enable the MAC address-table notification feature, set the interval time to e history-size to 100 entries:	
	Switch(config)# mac	address-table notification address-table notification interval 60 address-table notification history-size 100	

You can verify your settings by entering the show mac address-table notification privileged EXEC command.

Related Co

mands	Command	Description
	clear mac address-table notification	Clears the MAC address notification global counters.
	show mac address-table notification	Displays the MAC address notification settings on all interfaces or on the specified interface.
	snmp-server enable traps	Sends the SNMP MAC notification traps when the mac-notification keyword is appended.
	snmp trap mac-notification	Enables the SNMP MAC notification trap on a specific interface.

mac address-table static

Use the **mac address-table static** global configuration command to add static addresses to the MAC address table. Use the **no** form of this command to remove static entries from the table.

mac address-table static mac-addr vlan vlan-id interface interface-id

no mac address-table static mac-addr vlan vlan-id [interface interface-id]

Syntax Description	mac-addr	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
	vlan vlan-id	Specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.
	interface interface-id	Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.
Defaults	No static addresses are co	onfigured.
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Examples	-	to add the static address c2f3.220a.12f4 to the MAC address table. When a AN 4 with this MAC address as its destination, the packet is forwarded to the
Examples	packet is received in VLA specified interface:	
Examples	<pre>packet is received in VLA specified interface: Switch(config)# mac ad gigabitethernet0/1</pre>	AN 4 with this MAC address as its destination, the packet is forwarded to the
Examples Related Commands	<pre>packet is received in VLA specified interface: Switch(config)# mac ad gigabitethernet0/1</pre>	AN 4 with this MAC address as its destination, the packet is forwarded to the dress-table static c2f3.220a.12f4 vlan 4 interface

mac address-table static drop

Use the **mac address-table static drop** global configuration command to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the **no** form of this command to return to the default setting.

mac address-table static mac-addr vlan vlan-id drop

no mac address-table static mac-addr vlan vlan-id

Syntax Description	mac-addr	Unicast source or destination MAC address. Packets with this MAC address are dropped.
	vlan vlan-id	Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.
Defaults	Unicast MAC ad destination MAC	dress filtering is disabled. The switch does not drop traffic for specific source or C addresses.
Command Modes	Global configura	ation
Command History	Release	Modification
-	12.2(25)EX	This command was introduced.
Usage Guidelines	Follow these gui	delines when using this feature:
		AC addresses, broadcast MAC addresses, and router MAC addresses are not supported, are forwarded to the CPU are also not supported.
	the switch ei	unicast MAC address as a static address and configure unicast MAC address filtering, ther adds the MAC address as a static address or drops packets with that MAC address, n which command was entered last. The second command that you entered overrides the nd.
	interface-id	e, if you enter the mac address-table static <i>mac-addr</i> vlan <i>vlan-id</i> interface global configuration command followed by the mac address-table static <i>mac-addr</i> drop command, the switch drops packets with the specified MAC address as a source on.
		the mac address-table static <i>mac-addr</i> vlan <i>vlan-id</i> drop global configuration ollowed by the mac address-table static <i>mac-addr</i> vlan <i>vlan-id</i> interface <i>interface-id</i>

ExamplesThis example shows how to enable unicast MAC address filtering and to configure the switch to drop
packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in
VLAN 4 with this MAC address as its source or destination, the packet is dropped:
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 dropThis example shows how to disable unicast MAC address filtering:
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
You can verify your setting by entering the show mac address-table static privileged EXEC command.

Related Commands	Command	Description
	show mac address-table static	Displays only static MAC address table entries.

macro apply

Use the **macro apply** interface configuration command to apply a macro to an interface or to apply and trace a macro configuration on an interface.

macro {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

Syntax Description	apply	Apply a macro to the specified interface.	
	trace	Use the trace keyword to apply a macro to an interface and to debug the macro.	
	macro-name	Specify the name of the macro.	
	parameter value	(Optional) Specify unique parameter values that are specific to the interface. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.	
Defaults	This command has no default setting.		
Command Modes	Interface configuration		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	You can use the macro trace <i>macro-name</i> interface configuration command to apply and show the macros running on an interface or to debug the macro to find any syntax or configuration errors. If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the interface.		
	When creating a macro that requires the assignment of unique values, use the parameter value keywords to designate values specific to the interface.		
	Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.		
	Some macros might contain keywords that require a parameter value. You can use the macro apply <i>macro-name</i> ? command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.		
	When you apply a macro to an interface, the macro name is automatically added to the interface. You can display the applied commands and macro names by using the show running-configuration interface <i>interface-id</i> user EXEC command.		
	A macro applied to an interface range behaves the same way as a macro applied to a single interface. When you use an interface range, the macro is applied sequentially to each interface within the range. If a macro command fails on one interface, it is still applied to the remaining interfaces.		

You can delete a macro-applied configuration on an interface by entering the **default interface** *interface-id* interface configuration command.

Examples

After you have created a macro by using the **macro name** global configuration command, you can apply it to an interface. This example shows how to apply a user-created macro called **duplex** to an interface:

Switch(config-if) # macro apply duplex

To debug a macro, use the **macro trace** interface configuration command to find any syntax or configuration errors in the macro as it is applied to an interface. This example shows how troubleshoot the user-created macro called **duplex** on an interface:

Switch(config-if)# macro trace duplex Applying command...'duplex auto' %Error Unknown error. Applying command...'speed nonegotiate'

Related Commands

Command	Description
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 parser macro	Displays the macro definition for all macros or for the specified macro.

macro description

Use the **macro description** interface configuration command to enter a description about which macros are applied to an interface. Use the **no** form of this command to remove the description.

macro description *text*

no macro description text

Syntax Description	description <i>text</i> Enter a de	escription about the macros that are applied to the specified interface.	
Defaults	This command has no default	setting.	
Command Modes	Interface configuration		
Command History	Release Mo	dification	
	12.2(25)EX Thi	s command was introduced.	
Usage Guidelines	multiple macros are applied or	to associate comment text, or the macro name, with an interface. When n a single interface, the description text will be from the last applied macro dd a description to an interface:	
	This example shows how to add a description to an interface: Switch(config-if)# macro description duplex settings		
	You can verify your settings b command.	by entering the show parser macro description privileged EXEC	
Related Commands	Command	Description	
	macro apply	Applies a macro on an interface or applies and traces a macro on 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 parser macro	Displays the macro definition for all macros or for the specified	

macro global

Use the **macro global** global configuration command to apply a macro to a switch or to apply and trace a macro configuration on a switch.

macro global {apply | trace} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

Syntax Description	apply	Apply a macro to the switch.	
	trace	Apply a macro to a switch and to debug the macro.	
	macro-name	Specify the name of the macro.	
	parameter value	(Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.	
Defaults	This command has	s no default setting.	
Command Modes	Global configurati	on	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	macros running or If a command fails	acro trace <i>macro-name</i> global configuration command to apply and to show the a switch or to debug the macro to find any syntax or configuration errors. s because of a syntax error or a configuration error when you apply a macro, the macro or the remaining commands to the switch.	
	When creating a macro that requires the assignment of unique values, use the parameter <i>value</i> keywords to designate values specific to the switch.		
	Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.		
	Some macros might contain keywords that require a parameter value. You can use the macro global apply <i>macro-name</i> ? command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.		
	When you apply a macro to a switch, the macro name is automatically added to the switch. You can display the applied commands and macro names by using the show running-configuration user EXEC command.		
	You can delete a gi command containe	lobal macro-applied configuration on a switch only by entering the no version of each ed in the macro.	

Examples

After you have created a new macro by using the **macro name** global configuration command, you can apply it to a switch. This example shows how see the **snmp** macro and how to apply the macro and set the hostname to test-server and set the IP precedence value to 7:

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable
#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

To debug a macro, use the **macro global trace** global configuration command to find any syntax or configuration errors in the macro when it is applied to a switch. In this example, the **ADDRESS** parameter value was not entered, causing the snmp-server host command to fail while the remainder of the macro is applied to the switch:

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

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 description	Adds a description about the macros that are applied to the switch.
	macro name	Creates a macro.
	show parser macro	Displays the macro definition for all macros or for the specified macro.

macro global description

Use the **macro global description** global configuration command to enter a description about the macros that are applied to the switch. Use the **no** form of this command to remove the description.

macro global description *text*

no macro global description text

Syntax Description	description <i>text</i> Ent	er a description about the macros that are applied to the switch.
Defaults	This command has no c	default setting.
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
	This example shows ho Switch(config)# macro	plied on a switch, the description text will be from the last applied macro. we to add a description to a switch: o global description udld aggressive mode enabled tings by entering the show parser macro description privileged EXEC
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 name	Creates a macro.
		Displays the macro definition for all macros or for the specified macro.

macro name

Use the **macro name** global configuration command to create a configuration macro. Use the **no** form of this command to delete the macro definition.

macro name macro-name

no macro name macro-name

Syntax Description	n <i>macro-name</i> Name of the macro.			
Defective				
Defaults	This command ha	as no default setting.		
Command Modes	Global configuration			
Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
Usage Guidelines	A macro can contain up to 3000 characters. Enter one macro command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.			
	You can define mandatory keywords within a macro by using a help string to specify the keywords # macro keywords word to define the keywords that are available for use with the macro. You can up to three help string keywords separated by a space. If you enter more than three macro keyword the first three are shown.			
Macro names are case sensitive. For example, the commands macro name Sample-Macro name sample-macro will result in two separate macros.				
	When creating a macro, do not use the exit or end commands or change the command mode by usi interface <i>interface-id</i> . This could cause commands that follow exit , end , or interface <i>interface-id</i> execute in a different command mode.			
	those interfaces of an interface by en Alternatively, you	his command only deletes the macro definition. It does not affect the configuration of on which the macro is already applied. You can delete a macro-applied configuration on intering the default interface <i>interface-id</i> interface configuration command. u can create an <i>anti-macro</i> for an existing macro that contains the no form of all the ommands in the original macro. Then apply the anti-macro to the interface.		
	created macro ov	a macro by creating a new macro with the same name as the existing macro. The newly erwrites the existing macro but does not affect the configuration of those interfaces on al macro was applied.		

Examples

This example shows how to create a macro that defines the duplex mode and speed:

```
Switch(config)# macro name duplex
Enter macro commands one per line. End with the character `@'.
duplex full
speed auto
@
```

This example shows how create a macro with # macro keywords:

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

This example shows how to display the mandatory keyword values before you apply the macro to an interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# macro apply test ?
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
Switch(config-if)# macro apply test $VLANID ?
WORD Value of first keyword to replace
Switch(config-if)# macro apply test $VLANID 2
WORD keyword to replace with a value e.g $VLANID,$MAX
<cr>
Switch(config-if)# macro apply test $VLANID 2
WORD keyword to replace with a value e.g $VLANID,$MAX
```

WORD Value of second keyword to replace

Related Command	S
-----------------	---

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.
show parser macro	Displays the macro definition for all macros or for the specified macro.

match (access-map configuration)

Use the **match** access-map configuration command to set the VLAN map to match packets against one or more access lists. Use the **no** form of this command to remove the match parameters.

- **match** {**ip** address {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac** address {*name*} [*name*] [*name*]...}
- **no match** {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

Syntax Description	ip address	Set the access map to match packets against an IP address access list.	
	mac address	Set the access map to match packets against a MAC address access list.	
	name	Name of the access list to match packets against.	
	number	Number of the access list to match packets against. This option is not valid for MAC access lists.	
Defaults	The default act	tion is to have no match parameters applied to a VLAN map.	
Command Modes	Access-map configuration		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	You enter acces	ss-map configuration mode by using the vlan access-map global configuration command.	
	You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.		
	1	configuration mode, use the match command to define the match conditions for a VLAN a VLAN. Use the action command to set the action that occurs when the packet matches	
		tched only against access lists of the same protocol type; IP packets are matched against and all other packets are matched against MAC access lists.	
	Both IP and M	AC addresses can be specified for the same map entry.	

Examples This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *al2*.

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the show vlan access-map privileged EXEC command.

Related Commands	Command	Description
	access-list	Configures a standard numbered ACL. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands.
	action	Specifies the action to be taken if the packet matches an entry in an access control list (ACL).
	ip access list	Creates a named access list. 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	Creates a named MAC address access list.
	show vlan access-map	Displays the VLAN access maps created on the switch.
	vlan access-map	Creates a VLAN access map.

match access-group

Use the **match access-group** class-map configuration command to configure the match criteria for a class map on the basis of the specified access control list (ACL). Use the **no** form of this command to remove the ACL match criteria.

match access-group acl-index-or-name

no match access-group acl-index-or-name

Syntax Description	acl-index-or-name	Number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
Defaults	No match criteria are o	defined.
Command Modes	Class-map configurati	on
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	determine if packets b Before using the matc command to specify th	 pup command specifies a numbered or named ACL to use as the match criteria to elong to the class specified by the class map. ch access-group command, you must enter the class-map global configuration he name of the class whose match criteria you want to establish. h access-group classification only on input policy maps.
Examples	<pre>the match criterion: Switch(config)# class Switch(config-cmap) Switch(config-cmap);</pre>	ow to create a class map called in <i>class</i> , which uses the access control list <i>acl1</i> as ss-map match-any inclass # match access-group acl1 # exit ettings by entering the show class-map privileged EXEC command.
Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.
	show class-map	Displays quality of service (QoS) class maps.

match cos

Use the **match cos** class-map configuration command to match a packet based on a Layer 2 class of service (CoS) marking. Use the **no** form of this command to remove the CoS match criteria.

match cos cos-list

no match cos cos-list

Syntax Description	cos-list	List of up to four CoS values to match against incoming packets. Separate each value with a space. The range is 0 to 7.	
Defaults	No match criteria are	defined.	
Command Modes	Class-map configurat	ion	
Command History	Release	Modification	
-	12.2(25)EX	This command was introduced.	
Usage Guidelines	The match cos comm to the class specified	and specifies a CoS value to use as the match criteria to determine if packets belong by the class map.	
	Before using the match cos command, you must enter the class-map global configuration command to specify the name of the class whose match criteria you want to establish.		
	Matching of CoS values is supported only on ports carrying Layer 2 VLAN-tagged traffic. That is, you can use the cos classification only on IEEE 802.1Q trunk ports.		
	You can use match co	os classification in input and output policy maps.	
Examples	This example shows h CoS values of 1 and 4	ow to create a class map called in <i>class</i> , which matches all the incoming traffic with	
	Switch(config)# class-map match-any in-class Switch(config-cmap)# match cos 1 4 Switch(config-cmap)# exit		
	You can verify your s	ettings by entering the show class-map privileged EXEC command.	
Related Commands	Command	Description	
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.	
	show class-map	Displays quality of service (QoS) class maps.	

match ip dscp

Use the **match ip dscp** class-map configuration command to identify a specific IPv4 Differentiated Service Code Point (DSCP) value as match criteria for a class. Use the **no** form of this command to remove the match criteria.

match ip dscp dscp-list

no match ip dscp dscp-list

Syntax Description	ip-dscp-list	List of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You can also enter a mnemonic name for a commonly used value.	
		See the "Configuring QoS" chapter in the software configuration guide for this release for information about other options for specifying DSCP values.	
Defaults	No match criteria ar	e defined	
	i to materi criteria ai		
Command Modes	Class-map configura	ation	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines		command specifies a DSCP value to use as the match criteria to determine if packets	
	belong to the class specified by the class map. This command is used by the class map to identify a specific DSCP value marking on a packet. It context, DSCP values are used as markings only and have no mathematical significance. For example, the DSCP value of 2 is not greater than 1, but merely indicates that a packet marked with a value of different than one marked with a value of 1. You define the treatment of these marked packets by s QoS policies in policy-map class configuration mode.		
	Before using the match ip dscp command, you must enter the class-map global configuration command to specify the name of the class whose match criteria you want to establish.		
	You can enter up to eight DSCP values in one match statement. For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7, enter the match ip dscp 0 1 2 3 4 5 6 7 command. The packet must match only one (not all) of the specified IPv4 DSCP values to belong to the class.		
	You can use match ip dscp classification in input and output policy maps.		

Examples This example shows how to create a class map called in*class*, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

Switch(config)# class-map match-any in-class Switch(config-cmap)# match ip dscp 10 11 12 Switch(config-cmap)# exit

You can verify your settings by entering the show class-map privileged EXEC command.

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.
	show class-map	Displays quality of service (QoS) class maps.

match ip precedence

Use the **match ip precedence** class-map configuration command to identify IPv4 precedence values as match criteria for a class. Use the **no** form of this command to remove the match criteria.

match ip precedence ip-precedence-list

no match ip precedence ip-precedence-list

Syntax Description	ip precedence <i>ip-precedence-list</i>	List of up to four IPv4 precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7.	
Defaults	No match criteria are defined.		
Command Modes	Class-map configuration	on	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	The match ip precedence command specifies an IPv4 precedence value to use as the match criteria to determine if packets belong to the class specified by the class map.		
	The precedence values are used as marking only. In this context, the IP precedence values have no mathematical significance. For example, the precedence value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.		
	Before using the match ip precedence command, you must enter the class-map global confi command to specify the name of the class whose match criteria you want to establish.		
	IP precedence values of	ar IPv4 precedence values in one match statement. For example, if you wanted the of 0, 1, 2, or 7, enter the match ip precedence 0 1 2 7 command. The packet must II) of the specified IP precedence values to belong to the class.	
	You can use match ip	precedence classification in input and output policy maps.	
Examples	This example shows how to create a class map called <i>class</i> , which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:		
	-	ss-map match-any in-class # match ip precedence 5 6 7 # exit	
		ettings by entering the show class-map privileged EXEC command.	

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.
	show class-map	Displays quality of service (QoS) class maps.

match qos-group

Use the **match qos-group** class-map configuration command to identify a specific quality of service (QoS) group value as a match criterion for a class. Use the **no** form of this command to remove the match criterion.

match qos-group value

no match qos-group value

Syntax Description	qos-group value	A quality of service group value. The range is from 0 to 99.	
Defaults	No match criterion are defined.		
Command Modes	Class-map configurati	on	
Command History	Release	Modification	
-	12.2(25)EX	This command was introduced.	
	12.2(25)SEG	The QoS group range was extended to from 0 to 99.	
	 the precedence value of 2 is not greater than 1, but merely indicates that a packet marked of 2 is different than one marked with a value of 1. You define the treatment of these marked setting QoS policies in policy-map class configuration mode. The QoS-group value is local to the switch, meaning that the QoS-group value marked on a not leave the switch when the packet leaves the switch. If you require a marking that rema packet, use IP Differentiated Service Code Point (DSCP) values, IP precedence values, or method of packet marking. Before using the match qos-group command, you must enter the class-map global config command to specify the name of the class whose match criteria you want to establish. 		
		h qos-group classification only on output policy maps.	
		than 100 QoS groups on the switch (0 to 99).	
Examples	Switch(config)# cla Switch(config-cmap)	now to classify traffic by using QoS group 13 as the match criterion: ss-map match-any inclass # match qos-group 13	
	Switch(config-cmap)# exit You can verify your settings by entering the show class-map privileged EXEC command.		

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.
	show class-map	Displays QoS class maps.

mdix auto

Use the **mdix auto** interface configuration command to enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. Use the **no** form of this command to disable auto-MDIX. mdix auto no mdix auto Syntax Description This command has no arguments or keywords. Defaults Auto-MDIX is enabled. Command Modes Interface configuration **Command History** Release Modification 12.2(25)EX This command was introduced. **Usage Guidelines** When you enable auto-MDIX on an interface, you must also set the speed and duplex on the interface to auto so that the feature operates correctly. If the port is a user network interface (UNI), you must use the no shutdown interface configuration command to enable it before using the mdix auto command. UNIs are disabled by default. Network node interfaces (NNIs) are enabled by default. When auto-MDIX (along with autonegotiation of speed and duplex) is enabled on one or both of connected interfaces, link up occurs, even if the required cable type (straight-through or crossover) is not present. Auto-MDIX is supported on all 10/100-Mbps interfaces and on 10/100/1000BASE-T/BASE-TX small form-factor pluggable (SFP)-module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces. Examples This example shows how to enable auto-MDIX on a port: Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config-if) # speed auto Switch(config-if) # duplex auto Switch(config-if) # mdix auto Switch(config-if)# end You can verify the operational state of auto-MDIX on the interface by entering the show controllers

ethernet-controller interface-id phy privileged EXEC command.

Related Commands	Command	Description
	show controllers ethernet-controller interface-id phy	Displays general information about internal registers of an interface, including the operational state of auto-MDIX.

monitor session

Use the **monitor session** global configuration command to start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source or destination session, to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, and to limit (filter) SPAN source traffic to specific VLANs. Use the **no** form of this command to remove the SPAN or RSPAN session or to remove source or destination interfaces or filters from the SPAN or RSPAN session. For destination interfaces, the **encapsulation dot1q** or **encapsulation replicate** keywords are ignored with the **no** form of the command.

- **monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged**] **vlan** *vlan-id*}] | {**remote vlan** *vlan-id*}
- monitor session session_number filter vlan vlan-id [, | -]
- **monitor session** *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]} | {**remote vlan** *vlan-id*}
- **no monitor session** {*session_number* | **all** | **local** | **remote**}
- **no monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged**] **vlan** *vlan-id*}] | {**remote vlan** *vlan-id*}

no monitor session session_number filter vlan vlan-id [, | -]

no monitor session *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]} | {**remote vlan** *vlan-id*}

Syntax Description		
	session_number	Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 66.
	interface <i>interface-id</i>	Specify the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type and port number). For source interface , port channel is also a valid interface type, and the valid range is 1 to 48.
	destination	Specify the SPAN or RSPAN destination. A destination must be a physical port.
	encapsulation replicate	(Optional) Specify the encapsulation method. If not selected, the default is to send packets in native form (untagged).
		 dot1q—Specify IEEE 802.1Q encapsulation.
		• replicate —Specify that the destination interface replicates the source interface encapsulation method.
		Note Entering these keywords is valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore packets are always sent untagged.
	ingress	(Optional) Enable ingress traffic forwarding.
	dot1q vlan vlan-id	Specify ingress forwarding using IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN for ingress traffic.

untagged vlan vlan-id	Specify ingress forwarding using untagged encapsulation with the specified VLAN as the default VLAN for ingress traffic	
vlan vlan-id	When used with only the ingress keyword, set default VLAN for ingress traffic.	
remote vlan vlan-id	Specify the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094.	
	Note The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).	
,	(Optional) Specify a series of interfaces or VLANs, or separate a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.	
•	(Optional) Specify a range of interfaces or VLANs. Enter a space before and after the hyphen.	
filter vlan vlan-id	Specify a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The <i>vlan-id</i> range is 1 to 4094.	
source	Specify the SPAN or RSPAN source. A source can be a physical port, a port channel, or a VLAN.	
both, rx, tx	(Optional) Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.	
source vlan vlan-id	Specify the SPAN source interface as a VLAN ID. The range is 1 to 4094.	
all, local, remote	Specify all , local , or remote with the no monitor session command to clear all SPAN and RSPAN, all local SPAN, or all RSPAN sessions.	

Defaults

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

If **encapsulation dot1q** or **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

Command Modes Global configuration

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

Usage Guidelines

Traffic that enters or leaves source ports or source VLANs can be monitored by using SPAN or RSPAN. Traffic routed to source ports or source VLANs cannot be monitored.

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch.

You can have a maximum of 64 destination ports on a switch.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [, | -] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (-).

EtherChannel ports cannot be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

A private-VLAN port cannot be configured as a SPAN destination port.

You can monitor individual ports while they participate in an EtherChannel, or you can monitor the entire EtherChannel bundle by specifying the **port-channel** number as the RSPAN source interface.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x on a port that is a SPAN or RSPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination. (If IEEE 802.1x is not available on the port, the switch returns an error message.) You can enable IEEE 802.1x on a SPAN or RSPAN source port.

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session** *session_number* **filter vlan** *vlan-id* command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Destination ports can be configured to act in these ways:

- When you enter **monitor session** *session_number* **destination interface** *interface-id* with no other keywords, egress encapsulation is untagged, and ingress forwarding is not enabled.
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** with no other keywords, egress encapsulation replicates the source interface encapsulation; ingress forwarding is not enabled. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)

	• When you enter monitor session session_number destination interface interface-id encapsulation
	replicate ingress , egress encapsulation replicates the source interface encapsulation; ingress encapsulation depends on the keywords that follow— dot1q or untagged . (This applies to local SPAN only; RSPAN does not support encapsulation replication.)
	• When you enter monitor session <i>session_number</i> destination interface <i>interface-id</i> ingress , egress encapsulation is untagged; ingress encapsulation depends on the keywords that follow— dot1q or untagged .
Examples	This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on
-	source port 1 to destination port 2:
	<pre>Switch(config)# monitor session 1 source interface gigabitethernet0/1 both Switch(config)# monitor session 1 destination interface gigabitethernet0/2</pre>
	This example shows how to delete a destination port from an existing local SPAN session:
	<pre>Switch(config) # no monitor session 2 destination gigabitethernet0/2</pre>
	This example shows how to limit SPAN traffic in an existing session only to specific VLANs:
	<pre>Switch(config) # monitor session 1 filter vlan 100 - 304</pre>
	This example shows how to configure RSPAN source session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN 900.
	Switch(config)# monitor session 1 source interface gigabitethernet0/1 Switch(config)# monitor session 1 source interface port-channel 2 tx Switch(config)# monitor session 1 destination remote vlan 900 Switch(config)# end
	This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic.
	<pre>Switch(config)# monitor session 10 source remote vlan 900 Switch(config)# monitor session 10 destination interface gigabitethernet0/2</pre>
	This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.
	Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation replicate ingress dot1q vlan 5
	This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic replicates the source encapsulation; ingress traffic is untagged.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN and RSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Related Commands	Command	Description
	remote-span	Configures an RSPAN VLAN in vlan configuration mode.
	show monitor	Displays SPAN and RSPAN session information.
	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.

mvr (global configuration)

Use the **mvr** global configuration command without keywords to enable the multicast VLAN registration (MVR) feature on the switch. Use the command with keywords to set the MVR mode for a switch, configure the MVR IP multicast address, set the maximum time to wait for a query reply before removing a port from group membership, and to specify the MVR multicast VLAN. Use the **no** form of this command to return to the default settings.

mvr [group *ip-address* [count] | mode [compatible | dynamic] | querytime value | vlan vlan-id]

no mvr [group *ip-address* | mode [compatible | dynamic] | querytime *value* | vlan *vlan-id*]

Syntax Description	group ip-address	Statically configure an MVR group IP multicast address on the switch.
		Use the no form of this command to remove a statically configured IP multicast address or contiguous addresses or, when no IP address is entered, to remove all statically configured MVR IP multicast addresses.
	count	(Optional) Configure multiple contiguous MVR group addresses. The range is 1 to 256; the default is 1.
	mode	(Optional) Specify the MVR mode of operation.
		The default is compatible mode.
	compatible	Set MVR mode to provide compatibility with Catalyst 2900 XL and Catalyst 3500 XL switches. This mode does not allow dynamic membership joins on source ports.
	dynamic	Set MVR mode to allow dynamic MVR membership on source ports.
	querytime value	(Optional) Set the maximum time to wait for IGMP report memberships on a receiver port. This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR querytime for an IGMP group membership report before removing the port from multicast group membership.
		The value is the response time in units of tenths of a second. The range is 1 to 100; the default is 5 tenths or one-half second.
		Use the no form of the command to return to the default setting.
	vlan vlan-id	(Optional) Specify the VLAN on which MVR multicast data is expected to be received. This is also the VLAN to which all the source ports belong. The range is 1 to 4094; the default is VLAN 1.

Defaults

MVR is disabled by default.

The default MVR mode is compatible mode.

No IP multicast addresses are configured on the switch by default.

The default group ip address count is 0.

The default query response time is 5 tenths of or one-half second.

The default multicast VLAN for MVR is VLAN 1.

Command Modes Global configuration

Command History	Release	Modification	
·····,	12.2(25)EX	This command was introduced.	
Usage Guidelines	A maximum of 256	5 MVR multicast groups can be configured on a switch.	
	Use the mvr group command to statically set up all the IP multicast addresses that will take part in MVR. Any multicast data sent to a configured multicast address is sent to all the source ports on the switch and to all receiver ports that have registered to receive data on that IP multicast address.		
	MVR supports aliased IP multicast addresses on the switch. However, if the switch is interoperating with Catalyst 3550 or Catalyst 3500 XL switches, you should not configure IP addresses that alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).		
	The mvr querytim	e command applies only to receiver ports.	
	If the switch MVR multicast mode to	is interoperating with Catalyst 2900 XL or Catalyst 3500 XL switches, set the compatible.	
	When operating in	compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.	
	MVR can coexist v	vith IGMP snooping on a switch.	
Examples	This example show	rs how to enable MVR:	
	Switch(config)# 1	nvr	
	Use the show mvr groups.	privileged EXEC command to display the current setting for maximum multicast	
	This example show	s how to configure 228.1.23.4 as an IP multicast address:	
	Switch(config)# 1	nvr group 228.1.23.4	
	This example show 228.1.23.1 to 228.1	s how to configure ten contiguous IP multicast groups with multicast addresses from 1.23.10:	
	Switch(config)# 1	nvr group 228.1.23.1 10	
	Use the show mvr configured on the s	members privileged EXEC command to display the IP multicast group addresses witch.	
	This example show	s how to set the maximum query response time as one second (10 tenths):	
	Switch(config)# 1	nvr querytime 10	
	This example show	rs how to set VLAN 2 as the multicast VLAN:	
	Switch(config)# r	nvr vlan 2	
	You can verify you	r settings by entering the show mvr privileged EXEC command.	

Related Commands	Command	Description
	mvr (interface configuration)	Configures MVR ports.
	show mvr	Displays MVR global parameters or port parameters.
	show mvr interface	Displays the configured MVR interfaces with their type, mode, VLAN, status and Immediate Leave configuration, and can also displays all MVR groups of which the interface is a member.
	show mvr members	Displays all ports that are members of an MVR multicast group; if the group has no members, its status is shown as Inactive.

mvr (interface configuration)

Use the **mvr** interface configuration command to configure a Layer 2 port as a multicast VLAN registration (MVR) receiver or source port, to set the Immediate Leave feature, and to statically assign a port to an IP multicast VLAN and IP address. Use the **no** form of this command to return to the default settings.

mvr {**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* {[**group** *ip-address*] [**receiver vlan** *vlan-id*]}

no mvr {**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* {[**group** *ip-address*] [**receiver vlan** *vlan-id*]}}

Syntax Description	immediate	(Optional) Enable the Immediate Leave feature of MVR on a port. Use
	type	the no mvr immediate command to disable the feature. (Optional) Configure the port as an MVR receiver port or a source port.
	, pe	The default port type is neither an MVR source nor a receiver port. The no mvr type command resets the port as neither a source or a receiver port.
	receiver	Configure the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN.
	source	Configure the port as an uplink port that can send and receive multicast data for the configured multicast groups. All source ports on a switch belong to a single multicast VLAN.
		Note When you are configuring a trunk port as an MVR receiver port, we recommend that the source port is configured as a network node interface (NNI) and the MVR trunk receiver port is configured as a user node interface (UNI).
	vlan vlan-id	Specify the mvr vlan for the system.
	group ip-address	(Optional) Statically configure the specified MVR IP multicast group address for the specified multicast VLAN ID. This is the IP address of the multicast group that the port or VLAN is joining.
	receiver vlan vlan-id	(Optional) Specify a receiver VLAN.

Defaults

A port is configured as neither a receiver nor a source. The Immediate Leave feature is disabled on all ports.

No receiver port is a member of any configured multicast group.

Command Modes Interface configuration

Command History	Release	Modification		
	12.2(25)EX	This command was introduced.		
	12.2(25)SE	The receiver and <i>vlan-id</i> keywords were added. These are required to configure a trunk port as an MVR receiver port.		
Usage Guidelines	Configure a port as	a source port if that port should be able to both send and receive multicast data bound		
Usage Guidennes		multicast groups. Multicast data is received on all ports configured as source ports.		
	Receiver ports on a	a switch can be in different VLANs, but should not belong to the multicast VLAN.		
	A port that is not taking part in MVR should not be configured as an MVR receiver port or a source port. A non-MVR port is a normal switch port, able to send and receive multicast data with normal switch behavior.			
	When Immediate Leave is enabled, a receiver port leaves a multicast group more quickly. Without Immediate Leave, when the switch receives an IGMP leave message from a group on a receiver port, it sends out an IGMP MAC-based query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP MAC-based query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency.			
	The Immediate Leave feature should be enabled only on receiver ports to which a single receiver device is connected.			
	The mvr vlan group command statically configures ports to receive multicast traffic sent to the IP multicast address. A port statically configured as a member of group remains a member of the group until statically removed. In compatible mode, this command applies only to receiver ports; in dynamic mode, it can also apply to source ports. Receiver ports can also dynamically join multicast groups by using IGMP join messages.			
	When operating in	When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.		
	An MVR port can	not be a private-VLAN port.		
Examples	This example show	vs how to configure a port as an MVR receiver port:		
	J. 11 (11 J.)	interface gigabitethernet0/1)# mvr type receiver		
	Use the show mvr ports.	interface privileged EXEC command to display configured receiver ports and source		
	This example show	vs how to enable Immediate Leave on a port:		
	Switch(config)# Switch(config-if	interface gigabitethernet0/1)# mvr immediate		
	This example show	vs how to add a port on VLAN 1 as a static member of IP multicast group 228.1.23.4:		
		interface gigabitethernet0/2)# mvr vlan1 group 230.1.23.4		
	_	vs how to add a port 2 on VLAN 100 as a static member of IP multicast group example, the receive port is an access port:		
		interface gigabitethernet0/2)# mvr vlan 100 group 228.1.23.4		

This example shows how to add on port 5 the receiver VLAN 201 with an MVR VLAN of 100.

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 receiver vlan 201
```

This example shows how to add on port 5 the receiver VLAN 201 as a static member of the IP multicast group 239.1.1.1, with an MVR VLAN of 100:

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
```

You can verify your settings by entering the show mvr members privileged EXEC command.

Related Commands	Command	Description
	mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
	show mvr	Displays MVR global parameters or port parameters.
	show mvr interface	Displays the configured MVR interfaces or displays the multicast groups to which a receiver port belongs. Also displays all MVR groups of which the interface is a member.
	show mvr members	Displays all receiver ports that are members of an MVR multicast group.

pagp learn-method

Use the **pagp learn-method** interface configuration command to learn the source address of incoming packets received from an EtherChannel port. Use the **no** form of this command to return to the default setting.

pagp learn-method {aggregation-port | physical-port}

no pagp learn-method



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

Syntax Description	aggregation-port	Specify address learning on the logical port-channel. The switch sends packets to the source using any of the ports in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives.
	physical-port	Specify address learning on the physical port within the EtherChannel. The switch sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.
Defaults	The default is aggregation and the default is a solution and the second se	ation-port (logical port channel).
Command Modes	Interface configuratio	n
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines		er network interface (UNI), you must enter the port-type nni interface nd before configuring pagp learn-method . Learn must be configured to the same of the link.
Note	keyword is provided i port-priority interfac	supports address learning only on aggregate ports even though the physical-port n the command-line interface (CLI). The pagp learn-method and the pagp ce configuration commands have no effect on the switch hardware, but they are eroperability with devices that only support address learning by physical ports.

Note	When the link partner to the Cisco ME switch is a physical learner, we recommend that you configure the switch as a physical-port learner. Use the pagp learn-method physical-port interface configuration command, and set the load-distribution method based on the source MAC address by using the port-channel load-balance src-mac global configuration command. Only use the pagp learn-method interface configuration command in this situation.	
Examples	This example shows how to set the learning method to learn the address on the physical port within the EtherChannel: Switch(config-if) # pagp learn-method physical-port	
	This example shows how to set the learning method to learn the address on the port-channel within the EtherChannel: Switch(config-if)# pagp learn-method aggregation-port	
	You can verify your settings by entering the show running-config privileged EXEC command or the show pagp <i>channel-group-number</i> internal privileged EXEC command.	
Related Commands	CommandDescriptionpagp port-prioritySelects a port over which all traffic through the EtherChannel is sent.	

Displays PAgP channel-group information.

reference_list.html

the command.

Displays the operating configuration. For syntax information, use this link to

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_

Select the Cisco IOS Commands Master List, Release 12.2 to navigate to

the Cisco IOS Release 12.2 Command Reference listing page:

show pagp

show running-config

pagp port-priority

Use the **pagp port-priority** interface configuration command to select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. Use the **no** form of this command to return to the default setting.

pagp port-priority priority

no pagp port-priority

Note	PAgP is available only on network node interfaces (NNIs).		
Syntax Description	priority	A priority number ranging from 0 to 255.	
, ,	1 2	1 2 2 2	
Defaults	The default is 128.		
Command Modes	Interface configura	ation	
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines		user network interface (UNI), you must enter the port-type nni interface mand before configuring pagp port-priority .	
		with the highest operational priority and that has membership in the same e one selected for PAgP transmission.	
Note	keyword is provide port-priority inter	tch supports address learning only on aggregate ports even though the physical-port ed in the command-line interface (CLI). The pagp learn-method and the pagp face configuration commands have no effect on the switch hardware, but they are interoperability with devices that only support address learning by physical ports.	
	When the link partner to the Cisco ME switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the pagp learn-method physical-port interface configuration command and to set the load-distribution method based on the source MAC address by using the port-channel load-balance src-mac global configuration command. Use the pagp learn-method interface configuration command only in this situation.		

Examples This example shows how to set the port priority to 200:

Switch(config-if)# pagp port-priority 200

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

Related Commands	Command	Description
	pagp learn-method	Provides the ability to learn the source address of incoming packets.
	show pagp	Displays PAgP channel-group information.
	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_r eference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

permit (MAC access-list configuration)

Use the **permit** MAC access-list configuration command to allow non-IP traffic to be forwarded if the conditions are matched. Use the **no** form of this command to remove a permit condition from the extended MAC access list.

- {permit | deny} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
 dst-MAC-addr mask} [type mask | cos cos | aarp | amber | dec-spanning | decnet-iv |
 diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca / lsap lsap mask | mop-console |
 mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
- no {permit | deny} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | cos cos | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca / lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo |vines-ip | xns-idp]



Though visible in the command-line help strings, appletalk is not supported as a matching condition.

Syntax Description	any	Keyword to specify to deny any source or destination MAC address.
	host src-MAC-addr src-MAC-addr mask	Define a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
	host <i>dst-MAC-addr</i> <i>dst-MAC-addr</i> mask	Define a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
	type mask	(Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.
		• <i>type</i> is 0 to 65535, specified in hexadecimal.
		• <i>mask</i> is a mask of <i>don't care</i> bits applied to the Ethertype before testing for a match.
	aarp	(Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
	amber	(Optional) Select EtherType DEC-Amber.
	cos cos	(Optional) Select an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the cos option is configured.
	dec-spanning	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
	decnet-iv	(Optional) Select EtherType DECnet Phase IV protocol.
	diagnostic	(Optional) Select EtherType DEC-Diagnostic.
	dsm	(Optional) Select EtherType DEC-DSM.
	etype-6000	(Optional) Select EtherType 0x6000.
	etype-8042	(Optional) Select EtherType 0x8042.
	lat	(Optional) Select EtherType DEC-LAT.
	lavc-sca	(Optional) Select EtherType DEC-LAVC-SCA.

lsap lsap-number mask	(Optional) Use the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet.
	The <i>mask</i> is a mask of <i>don't care</i> bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Select EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Select EtherType DEC-MOP Dump.
msdos	(Optional) Select EtherType DEC-MSDOS.
mumps	(Optional) Select EtherType DEC-MUMPS.
netbios	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Select EtherType VINES IP.
xns-idp	(Optional) Select EtherType Xerox Network Systems (XNS) protocol suite.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in Table 2-3.

Table 2-3	IPX Filtering Criteria
-----------	------------------------

IPX Encapsulation Type		
Cisco IOS Name	Novell Name	Filter Criterion
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

Defaults This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes MAC access-list configuration

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

mac access-list extended

show access-lists

Usage Guidelines	You enter MAC access-list configuration mode by using the mac access-list extended global configuration command.		
	If you use the host keyword, you cannot enter an address mask; if you do not use the any or host keywords, you must enter an address mask.		
	After an access control entry (ACE) is added to an access control list, an implied deny-any-any condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.		
Note	For more information about MAC-named extended access lists, see the software configuration guide for this release.		
Examples	This example shows how to define the MAC-named extended access list to allow NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.		
	Switch(config-ext-macl) # permit any host 00c0.00a0.03fa netbios		
	This example shows how to remove the permit condition from the MAC-named extended access list:		
	Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios		
	This example permits all packets with Ethertype 0x4321:		
	Switch(config-ext-macl)# permit any any 0x4321 0		
	You can verify your settings by entering the show access-lists privileged EXEC command.		
Related Commands	Command Description		
	deny (MAC access-list configuration)Denies non-IP traffic to be forwarded if conditions are matched.		

Creates an access list based on MAC addresses for non-IP traffic.

Displays access control lists configured on a switch.

police

Use the **police** policy-map class configuration command to define an individual policer for classified traffic and to enter policy-map class police configuration mode. A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded. In policy-map class police configuration mode, you can specify multiple actions for a packet. Use the **no** form of this command to remove an existing policer.

police {rate-bps | cir cir-bps} [burst-bytes / bc [burst-value]] [conform-action [set-cos-transmit
 {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit
 {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-prec-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-qos-transmit
 qos-group-value | transmit] [exceed action [drop | set-cos-transmit {new-cos-value | [cos |
 dscp | precedence] [table table-map name]} | set-dscp-value | [cos |
 dscp | precedence] [table table-map name]} | set-dscp-transmit {new-cos-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} | set-gos-transmit {new-precedence-value | [cos |
 dscp | precedence] [table table-map name]} |
 set-gos-transmit {new-precedence-value | transmit]]

no police {rate-bps | cir cir-bps} [burst-bytes / bc [burst-value]] [conform-action
 [set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} |
 set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} |
 set-prec-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} |
 set-qos-transmit qos-group-value | transmit] [exceed action [drop | set-cos-transmit
 {new-cos-value | [cos | dscp | precedence] [table table-map name]} | set-dscp-transmit
 {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-dscp-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence] [table table-map name]} | set-gos-transmit
 {new-precedence-value | [cos | dscp | precedence]



When **police** is used with the **priority** policy-map class command for unconditionally rate-limiting the priority queue, burst size values are not supported, and the *rate-bps* range is smaller. Only the default conform-action of **transmit** and the default exceed-action of **drop** are supported.

Syntax Description	rate-bps	Specify the average traffic rate in bits per second (bps). The range is 8000 to 1000000000.	
		Note The range for police with the priority command for output service policies is 64000 to 1000000000.	
	cir	Committed information rate (CIR) used for policing traffic.	
	cir-bps	CIR rate in bps. The range is 8000 to 100000000 bps.	
		Note The range for police with the priority command for output service policies is 64000 to 1000000000.	
	burst-bytes	(Optional) Specify the normal burst size in bytes. The range is 8000 to 1000000.	
	bc [burst- value]	(Optional) Conform burst. The number of acceptable burst bytes. The range is 8000 to 1000000 bytes. If no burst value is entered, the system calculates a burst value that equals the number of bytes that can be sent in 250 milliseconds (ms) at the CIR rate. In most cases, the automatically calculated value is appropriate; enter a new value only if you are aware of all implications.	

conform-action	(Optional) Action to be taken for packets that conform to the CIR.	
set-cos-transmit new-cos-value	Set a new class of service (CoS) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.	
set-dscp-transmit new-dscp-value	Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DCSP value is 0 to 63.	
set-prec-transmit new-precedence-value	Set a new IP precedence value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.	
set-qos-transmit <i>qos-group-value</i>	Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new QoS value is 0 to 99.	
cos	(Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.	
dscp	(Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.	
precedence	(Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the <i>from-type</i> of the enhanced packet-marking action.	
table table-map name	(Optional) Used in conjunction with the preceding <i>from-type</i> keyword. Specify the table map to be used for the enhanced packet marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i> parameter of the action using this table map.	
transmit	(Optional) Send the packet unmodified.	
exceed action	(Optional) Action to be taken for packets that do not conform to the CIR.	
drop	Drop the packet.	

Defaults

No policers are defined. Conform burst (bc) is automatically configured to 250 ms at the configured CIR.

Command Modes Policy-map class configuration

Command History

Release	Modification
12.2(25)EX	This command was introduced.
12.2(25)SEG	Increased support for configuring conform and exceed actions. See "Usage Guidelines."

Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure conform-action marking using enhanced packet marking and configure exceed-action to send the packet unmodified, perform marking using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. This release also added support for the ability to mark multiple QoS parameters for the same class, and configure conform-action marking and exceed-action marking simultaneously.

The switch supports a maximum of 229 policer instances on the switch (228 user-configurable policers and 1 policer reserved for internal use). You can configure up to 46 policers on a port.

Policing is only supported in input policies or in output policies that were configured with the **priority** policy-map class configuration command to reduce bandwidth in the priority queue.

Note

When used with the **priority** command in an output policy, the police rate range is 64000 to 1000000000 bps, even though the range that appears in the command-line interface help is 8000 to 1000000000. You cannot attach an output service policy with an out-of-range rate.

An output policy map should match only the modified values of the out-of-profile traffic and not the original values.

To configure multiple conform-actions or multiple exceed-actions, enter policy-map class police configuration mode, and use the **conform-action** and **exceed-action** policy-map class police configuration commands.

When you define the policer and enter a carriage return, you enter policy-map class police configuration mode, which allows you to configure multiple policing actions. In this mode, these configuration commands are available:

- conform-action: the action to be taken on packets that conform to the CIR. The default action is to transmit the packet. For more information, see the conform-action policy-map class police command.
- **exceed-action**: the action to be taken on packets that do not conform to the CIR. The default action is to **drop** the packet. For more information, see the **exceed-action** policy-map class police command.
- exit: exits from QoS policy-map class police configuration mode. If you do not want to set multiple actions, you can enter exit without entering any other policy-map class police commands.
- **no**: negate or set the default values of a command.

Examples

This example shows how to configure a policer with a 1-Mbps average rate with a burst size of 20 KB. The policer sets a new DSCP precedence value if the packets conform to the rate and drops the packet if traffic exceeds the rate.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class inclass1
Switch(config-pmap-c)# police cir 1000000 20000 conform-action set-dscp-transmit 46
exceed-action drop
Switch(config-pmap-c)# exit
```

This example shows how to configure a policer with default actions.

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
conform-action	Define multiple actions for a policy-map class for packets that meet the CIR.
exceed-action	Define multiple actions for a policy-map class for packets that exceed the CIR.
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.

police aggregate (policy-map class configuration)

Use the **police aggregate** policy-map class configuration command to apply an aggregate policer to multiple classes in the same policy map. A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded. Use the **no** form of this command to remove the specified policer.

police aggregate aggregate-policer-name

no police aggregate aggregate-policer-name

Syntax Description	aggregate-policer-	name Name of the aggregate policer.	
Defaults	No aggregate police	ers are defined.	
Command Modes	Policy-map class co	onfiguration	
Command History	Release	Modification	
2	12.2(25)EX	This command was introduced.	
Usage Guidelines	The switch supports a maximum of 229 policer instances on the switch (228 user-configurable policers and 1 policer reserved for internal use). You can configure up to 46 policers on a port.		
	Aggregate policing applies only to input policy maps.		
	An aggregate policer differs from an individual policer in that it is shared by multiple traffic classes within a policy map. You use an aggregate policer to police traffic streams across multiple classes in a policy map attached to an interface. You cannot use aggregate policing to aggregate traffic streams across multiple interfaces.		
	Only one policy ma	p can use any specific aggregate policer.	
Examples	This example shows classes on the same	s how to configure the aggregate policing with default actions and apply it across all port:	
	Switch(config-pma Switch(config-pma Switch(config-pma Switch(config-pma Switch(config-pma Switch(config-pma	p)# class in-class2 p-c)# police aggregate agg_policer1	
	Switch(config-pma	-	
	You can verify your	r settings by entering the show aggregate policer 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 policer aggregate	Displays the aggregate policer configuration.

policer aggregate (global configuration)

Use the **policer aggregate** global configuration command to create an aggregate policer to police all traffic across multiple classes in an input policy map. An aggregate policer can be shared by multiple classes in the same policy map. A policer defines a maximum permissible rate of transmission or committed information rate, a maximum burst size for transmissions, and an action to take if the maximum is met or exceeded. Use the **no** form of this command to remove the specified policer.

policer aggregate aggregate-policer-name {rate-bps | cir cir-bps } [bc burst- value]
 [conform-action [set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table
 table-map name] } | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table
 table-map name] } | set-prec-transmit {new-precedence-value | [cos | dscp | precedence]
 [table table-map name] } | set-qos-transmit qos-group-value | transmit] [exceed action [drop
 | set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name] } |
 set-dscp-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name] } |
 set-gos-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name] } |
 set-gos-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name] } |

no policer aggregate aggregate-policer-name {rate-bps | cir cir-bps} [bc burst- value]
 [conform-action [set-cos-transmit {new-cos-value | [cos | dscp | precedence] [table
 table-map name]} | set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table
 table-map name]} | set-prec-transmit {new-precedence-value | [cos | dscp | precedence]
 [table table-map name]} | set-qos-transmit qos-group-value | transmit] [exceed action [drop
 | set-dscp-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} |
 set-dscp-transmit {new-cos-value | [cos | dscp | precedence] [table table-map name]} |
 set-dscp-transmit {new-dscp-value | [cos | dscp | precedence] [table table-map name]} |
 set-gos-transmit {new-precedence-value | [cos | dscp | precedence] [table table-map name]} |

aggregate-policer-name	Name of the aggregate policer.
rate-bps	Specify the average traffic rate in bits per second (bps). The range is 8000 to 1000000000.
cir cir-bps	Committed information rate (CIR) in bits per second. The range is 8000 to 1000000000 bps.
bc burst- value	(Optional) Conform burst. The number of acceptable burst bytes. The range is 8000 to 1000000 bytes. If no burst value is entered, the system calculates a burst value that equals the number of bytes that can be sent in 250 milliseconds (ms) at the CIR rate. In most cases, the automatically calculated value is appropriate; enter a new value only if you are aware of all implications.
conform-action	(Optional) Action to be taken on packets that conform to the CIR.
set-cos-transmit cos-value	Set a new class of service (CoS) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new CoS value is 0 to 7.
set-dscp-transmit dscp-value	Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new DCSP value is 0 to 63.
set-prec-transmit precedence-value	Set a new IP precedence value for the packet and send the packet. This specifies the <i>to-type</i> of the marking action. The range for the new IP precedence value is 0 to 7.
	rate-bps cir cir-bps bc burst- value conform-action set-cos-transmit cos-value set-dscp-transmit dscp-value set-prec-transmit

	parameter of the action using this table map.
	marking. The <i>to-type</i> of the action is marked based on the <i>from-type</i>
	keyword. Specify the table map to be used for the enhanced packet
table table-map name	(Optional) Used in conjunction with the preceding from-type
	action.
	packet. This specifies the from-type of the enhanced packet-marking
	based on the IP precedence value of the incoming packet, and send th
precedence	(Optional) Set the packet marking specified in the preceding keywor
	This specifies the <i>from-type</i> of the enhanced packet-marking action
	based on the DSCP value of the incoming packet, and send the packet
dscp	(Optional) Set the packet marking specified in the preceding keywor
	This specifies the <i>from-type</i> of the enhanced packet-marking action
	based on the CoS value of the incoming packet, and send the packet
cos	(Optional) Set the packet marking specified in the preceding keywor
000	
	for the new QoS value is 0 to 99.
set-qos-transmit qos-group-value	Set a new quality of service (QoS) group value for the packet and sen the packet. This specifies the <i>to-type</i> of the marking action. The rang

Defaults

No aggregate policers are defined.

When you configure an aggregate policer, conform burst (**bc**) is automatically configured at 250 ms at the configured CIR.

Command Modes Global configuration

Release Modification 12.2(25)EX This command was introduced. 12.2(25)SEG Increased support for configuring conform and exceed actions. See "Usage Guidelines."

Usage Guidelines Beginning with Cisco IOS Release 12.2(25)SEG, you can configure conform-action marking using enhanced packet marking and configure exceed-action to send the packet unmodified, perform marking using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. This release also added support for the ability to mark multiple QoS parameters for the same class, and configure conform-action marking and exceed-action marking simultaneously.

The switch supports a maximum of 256 unique aggregate policer.s.

Aggregate policing is supported only in input policy maps.

You can configure multiple conform and exceed actions simultaneously for an aggregate policer as parameters in the **policer aggregate** global configuration command, but you must enter the actions in this order:

- conform-action must be followed by transmit or by set actions in this order:
 - set-qos-transmit
 - set-dscp-transmit or set-prec-transmit
 - set-cos-transmit
- exceed-action must be followed by drop or transmit or by set actions in this order:
 - set-qos-transmit
 - set-dscp-transmit or set-prec-transmit
 - set-cos-transmit

An output policy map should match only the modified values of the out-of-profile traffic and not the original values.

When you configure an aggregate policer, you can configure specific burst sizes and conform and exceed actions. If burst size (**bc**) is not specified, the system calculates an appropriate burst size value that equals the number of bytes that can be sent in 250 ms at the CIR rate. In most cases, the automatically calculated value is appropriate; enter a new value only if you are aware of all implications.

Examples This example shows how to configure an aggregate policer named *agg-pol-1* and attach it to multiple classes within a policy map:

Switch(config) # policer aggregate agg-pol-1 10900000 80000 exceed-action drop Switch(config)# class-map test1 Switch(config-cmap)# match access-group 1 Switch(config-cmap)# exit Switch(config)# class-map test2 Switch(config-cmap)# match access-group 2 Switch(config-cmap)# exit Switch(config) # policy map testexample Switch(config-pmap)# class test1 Switch(config-pmap-c)# police aggregate agg-pol-1 Switch(config-cmap-c)# exit Switch(config-pmap)# class test2 Switch(config-pmap-c)# police aggregate agg-pol-1 Switch(config-pmap-c)# exit Switch(config-9map) # exit Switch(config)# interface fastethernet0/1 Switch(config-if)# service-policy input testexample Switch(config-if)# exit

You can verify your settings by entering the show aggregate-policer 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 policer aggregate	Displays the aggregate policer configuration.

policer cpu uni

Use the **policer cpu uni** global configuration command to configure the CPU policing threshold for all user network interfaces (UNIs) on the switch. Use the **no** form of this command to return to the default.

policer cpu uni *rate-bps*

no policer cpu uni

Syntax Description	rate-bps	Specify the CPU policing threshold in bits per second (bps). The range is 8000 to 409500.	
Defaults	The default policing	threshold is 160000 bps.	
Command Modes	Global configuration		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	To protect against accidental or intentional CPU overload, the Cisco ME switch automatically provides control-plane security by dropping or rate-limiting a predefined set of Layer 2 control packets and some Layer 3 control packets for UNIs. The switch pre-allocates 27 control-plane security policers for CPU protection, numbered 0 to 26. A policer of 26 means a drop policer. A policer of a value of 0 to 25 means that a rate-limiting policer is assigned to the port for the control protocol.		
		-allocated. You can configure only the rate-limiting threshold by using the policer mand. The configured threshold applies to all control protocols and all UNIs.	
	For more information	a about control-plane security, see the software configuration guide for this release.	
Examples	Switch# config t	-	
	You can verify your s	settings by entering the show policer cpu uni rate privileged EXEC command.	
Related Commands	Command	Description	
	show policer cpu un	ii rate Displays configured policer threshold for control-plane security.	

policy-map

Use the **policy-map** global configuration command to create or to modify a policy map that can be attached to multiple physical ports and to enter policy-map configuration mode. Use the **no** form of this command to delete an existing policy map.

policy-map policy-map-name

no policy-map *policy-map-name*

Syntax Description	policy-map-name	Name of the policy map.	
Defaults	No policy maps are de	efined. By default, packets are sent unmodified.	
Command Modes	Global configuration		
Command History	Release	Modification	
	12.2(25)EX	This command was introduced.	
Usage Guidelines	The switch supports a	maximum of 256 unique policy maps.	
	Before configuring policies for classes whose match criteria are defined in a class map, use the policy-map command to specify the name of the policy map to be created or modified. Entering the policy-map command also enables the policy-map configuration mode, in which you can configure or modify the class policies for that policy map.		
	After entering the policy-map command, you enter policy-map configuration mode, and these configuration commands are available:		
	• class : the specified traffic classification for which the policy actions are applied. The classification is defined in the class-map global configuration command. For more information, see the class-map command.		
	• description : desc	cribes the policy map (up to 200 characters).	
	• exit: exits policy-map configuration mode and returns to global configuration mode.		
	• no : removes a previously defined policy map.		
	You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the class-map global configuration and match class-map configuration commands. You define packet classification on a physical-port basis.		
		policy maps and output policy maps, and you can assign one input policy map and to a port. The input policy map acts on incoming traffic on the port; the output tgoing traffic.	
	You can apply the can	ne policy man to multiple physical ports	

You can apply the same policy map to multiple physical ports.

Follow these guidelines when configuring input policy maps:

- The total number of input policy maps that can be attached to interfaces on the switch is limited by the availability of hardware resources. If you attempt to attach an input policy map that would exceed any hardware resource limitation, the configuration fails.
- An input policy map can contain a maximum of 32 class maps.
- You cannot configure an IP (IP standard and extended ACL, DSCP or IP precedence) and a non-IP (MAC ACL or CoS) classification within the same policy map, either within a single class map or across class maps within the policy map.
- After you use the **service-policy input** policy-map configuration command to attach an input policy map to an interface, you can modify the policy without detaching it from the interface. You can add or delete classification criteria, classes, or actions, or change the parameters of the configured actions (policers, rates, mapping, marking, and so on).
- These commands are not supported on input policy maps: **match qos-grou**p command, **bandwidth** command for Class-Based-Weighting-Queuing (CBWFQ), **priority** command for class-based priority queueing, **queue-limit** command for Weighted Tail Drop (WTD), **shape average** command for port shaping, or class-based traffic shaping.

Follow these guidelines when configuring output policy maps:

- Output policy maps can have a maximum of four classes, one of which is the class-default.
- Beginning with Cisco IOS Release 12.2(35)SE, the switch supports configuration and attachment of a unique output policy map for each port on the switch. However, these output policy maps can contain only three configurations of queue limits. You can include these three unique queue-limit configurations in as many output policy maps as there are switch ports. If you try to attach an output policy map that has a fourth queue-limit configuration, you see an error message, and the attachment is not allowed. There are no limitations on the configurations of bandwidth, priority, or shaping.
- All output policy maps must include the same number of class maps (one to three) and the same classification (that is, the same class maps).
- After you have attached a output policy map to an interface by using the **service-policy output** interface configuration command, you can only change the parameters of the configured actions (rates, percentages, and so on) or add or delete classification criteria of the class map while the policy map is attached to the interface. To add or delete a class or an action, you must detach the policy map from all interfaces, change it, and then reattach it to interfaces.
- These commands are not supported on output policy maps: **match access-group** command, **set** command for marking, and **police** command for policing without including the **priority** command.

For more information about policy maps, see the software configuration guide for this release.

Examples

This example shows how to create an input policy map for three classes:

```
Switch(config)# policy-map input-all
Switch(config-pmap)# class gold
Switch(config-pmap-c)# set dscp af43
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# police 20000000
```

L

This example shows how to configure an output policy map that provides priority with rate limiting to the gold class and guarantees a minimum remaining bandwidth percent of 20 percent to the silver class and 10 percent to the bronze class:

```
Switch(config)# policy-map output-2
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
```

This example shows how to delete the policy map *output-2*:

Switch(config) # no policy-map output-2

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.
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.
	service-policy (interface configuration)	Applies a policy map to a port.
	show policy-map	Displays quality of service (QoS) policy maps.

port-channel load-balance

Use the **port-channel load-balance** global configuration command to set the load-distribution method among the ports in the EtherChannel. Use the **no** form of this command to return to the default setting.

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port-channel load-balance

Syntax Description	dst-ip	Load distribution is based on the destination host IP address.
	dst-mac	Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
	src-dst-ip	Load distribution is based on the source and destination host IP address.
	src-dst-mac	Load distribution is based on the source and destination host MAC address.
	src-ip	Load distribution is based on the source host IP address.
	src-mac	Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
Defaults	The default is	src-mac.
Command Modes	Global config	uration
Command History	Release	Modification
	12.2(25)EX	This command was introduced.
Usage Guidelines	For information about when to use these forwarding methods, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.	
Examples	This example	shows how to set the load-distribution method to dst-mac:
	Switch(config	g)# port-channel load-balance dst-mac
	•	y your setting by entering the show running-config privileged EXEC command or the annel load-balance privileged EXEC command.

Related Commands	Command	Description
	interface port-channel	Accesses or creates the port channel.
	show etherchannel	Displays EtherChannel information for a channel.
	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_comman d_reference_list.html Select the Cisco IOS Commands Master List, Release 12.2 to navigate to the command.

port-type

Use the **port-type** interface configuration command to change the port type on a Cisco ME switch from a network node interface (NNI) to a user network interface (UNI) or the reverse. Use the **no** form of this command to return to the default setting of UNI.

port-type {uni | nni}

no port-type

Syntax Description	uni	User network interface.
	nni	Network node interface.
Defaults		iguration file exists, all the 10/100 ports on the Cisco ME switch are UNIs, and the small or pluggable (SFP) module slots on the Cisco ME switch are NNIs.
	to other po command	It status for a UNI is administratively down to prevent unauthorized users from gaining access orts as you configure the switch. You must use the no shutdown interface configuration to enable a UNI before you can configure it. The default status for an NNI is administratively w a service provider remote access to the switch during initial configuration.
Command Modes	Interface c	configuration
Command History	Release	Modification
	12.2(25)E	X This command was introduced.
Usage Guidelines	interface t	be reconfigured from UNI to NNI and the reverse. When a port is reconfigured as the other ype, it inherits all the characteristics of that interface type. At any time, all ports on the switch are either UNI or NNI.
	Some features are supported only on one port type (UNI or NNI). For information about specific feature support, see the software configuration guide for this release. When you change a port from an NNI to a UNI (or from a UNI to an NNI), any features exclusive to a port type are removed from the configuration to prevent conflicting configuration options on a specific interface. Every port on the switch can be a UNI, but only four ports can be NNIs at the same time. When you use the no port-type command on any interface, whether it is currently a UNI or an NNI, the interface defaults to UNI.	
	Traffic is not switched between UNIs, and all traffic incoming on UNIs must exit on NNIs to prevent a user from gaining access to another user's private network. If it is appropriate for two or more UNIs to exchange traffic within the switch, the UNI can be assigned to a community VLAN. For more information about configuring VLANs, see the software configuration guide for this release.	

ExamplesThis example shows how to change a port from a UNI to an NNI.Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type nni
5d20h: %SYS-5-CONFIG_I: Configured from console by console
Switch(config-if)# end
Switch# copy running-config startup-config

This example shows how to change a port back to a UNI.

Switch# config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface fastethernet0/1 Switch(config-if)# port-type uni Switch(config-if)# end

Related Commands	Command	Description
	no shutdown	Enables an interface.
	show interfaces	Displays the statistical information specific to all interfaces or to a specific interface.
	show port-type	Displays the port type of an interface.

Use the **priority** policy-map class configuration command to configure class-based priority queuing for a class of traffic belonging to an output policy map. The switch supports strict priority queuing or priority used with the **police** policy-map command. Use the **no** form of this command to remove a priority specified for a class.

priority

no priority

Note

When the **police** command is used with the **priority** policy-map class command for unconditionally rate-limiting the priority queue, burst size values are not supported for the **police** command.

Syntax Description This command has no arguments or keywords.

Defaults No policers are defined.

Command Modes Policy-map class configuration

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

Usage Guidelines

When used by itself (not followed by the **police** policy-map command), the **priority** command assigns traffic to a low-latency path and ensures that packets belonging to the class have the lowest possible latency. With strict priority queuing, packets in the priority queue are scheduled and sent until the queue is empty.

Note

You should exercise care when using the **priority** command without the **policy** command. Excessive use of strict priority queuing might cause congestion in other queues.

You can use **priority** with the **police** {*rate-bps* | **cir** *cir-bps*} policy-map command to reduce the bandwidth used by the priority queue. This is the only form of policing that is supported in output policy maps. Using this combination of commands configures a maximum rate on the priority queue and allows you to use the **bandwidth** and **shape average** policy-map commands for other classes to allocate traffic rates on other queues.



When you use the **police** command with the **priority** command in an output policy, the police rate range is 64000 to 1000000000 bps, even though the range that appears in the command-line help is 8000 to 1000000000. Configured burst size is ignored when you try to attach the output service policy.

Г

When you configure priority in an output policy map without the **police** command, you can only configure the other queues for sharing by using the **bandwidth remaining percent** policy-map class command. This command does not guarantee the allocated bandwidth, but the rate of distribution.

When you configure priority in an output policy map with the **police** command, you can configure other queues for sharing by using the **bandwidth** policy-map class command and for shaping by using the **shape average** policy-map class command.

You can associate the **priority** command only with a single unique class for all attached output policies on the switch.

You cannot associate the **priority** command with the **class-default** of the output policy map.

You cannot configure priority and any other scheduling action (**shape average** or **bandwidth**) in the same class.

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

Examples

This example shows how to configure the class *out-class1* as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that *out-class-2* gets 50 percent of the remaining bandwidth and *out-class3* gets 20 percent of the remaining bandwidth. The class **class-default** receives the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

This example shows how to use the **priority** with **police** commands to configure *out-class1* as the priority queue, with traffic going to the queue limited to 20000000 bits per second (bps) so that the priority queue never uses more than that. Traffic above that rate is dropped. The other traffic queues are configured as in the previous example.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# exit
Switch(config-jmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# 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.
	police	Defines a policer for classified traffic.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	show policy-map	Displays quality of service (QoS) policy maps.

private-vlan

Use the **private-vlan** VLAN configuration command to configure private VLANs and to configure the association between private-VLAN primary and secondary VLANs. Use the **no** form of this command to return the VLAN to normal VLAN configuration.

private-vlan {association [add | remove] secondary-vlan-list | community | isolated | primary}

no private-vlan {association | community | isolated | primary}

Syntax Description	association	Create an association between the primary VLAN and a secondary VLAN.	
	secondary-vlan-list	Specify one or more secondary VLANs to be associated with a primary VLAN in a private VLAN.	
	add	Associate a secondary VLAN to a primary VLAN.	
	remove	Clear the association between a secondary VLAN and a primary VLAN.	
	community	Designate the VLAN as a community VLAN.	
	isolated	Designate the VLAN as a community VLAN.	
	primary	Designate the VLAN as a community VLAN.	
Defaults	The default is to no co	nfigured private VLANs.	
Command Modes	VLAN configuration		
Command History	Release	Modification	
,	12.2(25)EX	This command was introduced.	
Usage Guidelines		figure private VLANs on all switches in the Layer 2 network to merge their Layer vent flooding of private-VLAN traffic.	
	You cannot include VLAN 1 or VLANs 1002 to 1005 in the private-VLAN configuration. Extended VLANs (VLAN IDs 1006 to 4094) can be configured as private VLANs.		
	You can associate a secondary (isolated or community) VLAN with only one primary VLAN. A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it.		
	• A secondary VLAN cannot be configured as a primary VLAN.		
	• The <i>secondary_vlan_list</i> parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.		
	• If you delete either the primary or secondary VLANs, the ports associated with the VLAN become inactive.		

A **community** VLAN carries traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN. A community VLAN can include no more than eight user network interfaces (UNIs).

An **isolated** VLAN is used by isolated ports to communicate with promiscuous ports. It does not carry traffic to other community ports or to isolated ports with the same primary VLAN domain.

A **primary** VLAN is the VLAN that carries traffic from a gateway to customer end stations on private ports.

The private-vlan commands do not take effect until you exit from VLAN configuration mode.

Do not configure private-VLAN ports as EtherChannels. While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.

A private VLAN cannot be a Remote Switched Port Analyzer (RSPAN) VLAN.

A private VLAN cannot be a user network interface (UNI) VLAN. If the VLAN is a UNI isolated VLAN (the default), you can change it to a private VLAN by entering the **private-vlan** VLAN configuration command. If a VLAN has been configured as a UNI community VLAN, you must first enter the **no uni-vlan** VLAN configuration command before configuring it as a private VLAN.

Although a private VLAN contains more than one VLAN, only one STP instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.

See the **switchport private-vlan** command for information about configuring host ports and promiscuous ports.

Note

For more information about private-VLAN interaction with other features, see the software configuration guide for this release.

Examples

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, VLANs 502 and 503 as community VLANs, and to associate them in a private VLAN. The example assumes that VLANs 502 and 503 were previously configured as UNI community VLANs.

```
Switch# configure terminal
Switch(config) # vlan 20
Switch(config-vlan) # private-vlan primary
Switch(config-vlan)# exit
Switch(config) # vlan 501
Switch(config-vlan) # private-vlan isolated
Switch(config-vlan)# exit
Switch(config) # vlan 502
Switch(config-vlan) # no uni-vlan
Switch(config-vlan) # private-vlan community
Switch(config-vlan) # exit
Switch(config) # vlan 503
Switch(config-vlan) # no uni-vlan
Switch(config-vlan) # private-vlan community
Switch(config-vlan)# exit
Switch(config) # vlan 20
Switch(config-vlan) # private-vlan association 501-503
Switch(config-vlan) # end
```

You can verify your setting by entering the **show vlan private-vlan** or **show interfaces status** privileged EXEC command.

Related Commands	Command	Description
	show interfaces status	Displays the status of interfaces, including the VLANs to which they belong.
	show vlan private-vlan	Displays the private VLANs and VLAN associations configured on the switch.
	switchport private-vlan	Configures a private-VLAN port as a host port or promiscuous port.

queue-limit

Use the **queue-limit** policy-map class configuration command to set the queue maximum threshold for Weighted Tail Drop (WTD) in an output policy map. Use the **no** form of this command to return to the default.

- **queue-limit** [cos value | dscp value | precedence value | qos-group value] number-of-packets [packets]
- **no queue-limit** [cos value | dscp value | precedence value | qos-group value] number-of-packets [packets]

Syntax Description	cos value	(Optional) Set the parameters for each cost of service (CoS) value. The range is from 0 to 7.
	dscp value	(Optional) Set the parameters for each Differentiated Services Code Point (DSCP) value. The range is from 0 to 63.
	precedence value	(Optional) Set the parameters for each IP precedence value. The range is from 0 to 7.
	qos-group value	(Optional) Set the parameters for each quality-of-service (QoS) group value. The range is from 0 to 99.
	number-of-packets [packets]	Set the maximum threshold for WTD as the number of packets in the queue. The range is from 16 to 544 and refers to 256-byte packets. The default is 48 packets. The packets keyword is optional.
		Note For optimal network performance, we strongly recommend that you configure the maximum queue-limit to 272 or less.
Defaults	Default queue limit is	48 (256-byte) packets.
Command Modes	Policy-map class confi	guration
Command History	Release	Modification
	12.2(25)EX	This command was introduced.

()	
12.25(SEG)	Support was added to configure the queue-limit in the class-default of an output policy map.
	output poney mup.

Usage Guidelines You use the **queue-limit** policy-map class command to control output traffic. Queue-limit settings are not supported in input policy maps. Beginning with Cisco IOS Release 12.2(35)SE, the switch supports one output policy map for each interface. However the limit of three unique queue-limit configurations across all output policy maps remains in effect You can use the same queue-limit configuration across multiple policy maps. Within an output policy map only four queues (classes) are allowed, including the class default. Each queue has three defined thresholds (queue limits). Only three queue-limit configurations are allowed on the switch, but multiple policy maps can share the same queue-limits. For two policy maps to share a queue-limit configuration, all threshold values must be the same for all classes in both policy maps. If you try to attach an output policy map that contains a fourth queue-limit configuration to an interface, you see an error message and the attachment is not allowed. The queue-limit command is supported only after you first configure a scheduling action, such as bandwidth, shape-average, or priority, except when you configure queue-limit in the class-default of an output policy map. You cannot configure more than two unique threshold values for WTD qualifiers (cos, dscp, precedence, or qos-group) in the queue-limit command. However, you can map any number of qualifiers to those thresholds. You can configure a third unique threshold value to set the maximum queue, using the queue-limit command with no qualifiers. When you use the **queue-limit** command to configure thresholds within a class map, the WTD thresholds must be less than or equal to the maximum threshold of the queue. This means that the queue size configured without a qualifier must be larger than any of the queue sizes configured with a qualifier. Examples This example shows how to configure WTD so that out-class1, out-class2, out-class3, and class-default get a minimum of 40, 20, 10 and 10 percent of the traffic bandwidth respectively. The corresponding queue-sizes are set to 48, 32, 16 and 272 (256-byte) packets: Switch(config)# policy-map out-policy Switch(config-pmap)# class outclass1 Switch(config-pmap-c)# bandwidth percent 40 Switch(config-pmap-c)# queue-limit 48 Switch(config-pmap-c)# exit Switch(config-pmap)# class outclass2 Switch(config-pmap-c)# bandwidth percent 20 Switch(config-pmap-c)# queue-limit 32 Switch(config-pmap-c)# exit Switch(config-pmap)# class outclass3 Switch(config-pmap-c)# bandwidth percent 10 Switch(config-pmap-c)# queue-limit 16 Switch(config-pmap-c)# exit Switch(config-pmap)# class class-default Switch(config-pmap-c)# bandwidth percent 10 Switch(config-pmap-c)# queue-limit 272

Switch(config-pmap-c)# exit Switch(config-pmap)# exit Switch(config)# interface gigabitethernet 0/1 Switch(config-if)# service-policy output out-policy Switch(config-if)# exit This example shows how to configure WTD for a Fast Ethernet port where *outclass1*, *outclass2*, and *outclass3* get a minimum of 50, 20, and 10 percent of the traffic bandwidth. The **class-default** gets the remaining 20 percent. Each corresponding queue size is set to 64, 32, and 16 (256-byte) packets, respectively. The example also shows how if *outclass1* matches to dscp 46, 56, 57, 58, 60, 63, a DSCP value of 46 gets a queue size of 32 (256-byte) packets; DSCP values 56, 57, and 58 get queue sizes of 48 (256-byte) packets; and the remaining DSCP values of 60 and 63 get the default queue size of 64 (256-byte) packets.

```
Switch(config) # policy-map out-policy
Switch(config-pmap) # class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 64
Switch(config-pmap-c)# queue-limit dscp 46 32
Switch(config-pmap-c)# queue-limit dscp 56 48
Switch(config-pmap-c)# queue-limit dscp 57 48
Switch(config-pmap-c)# queue-limit dscp 58 48
Switch(config-pmap-c)# exit
Switch(config-pmap) # class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap) # class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if) # service-policy output out-policy
Switch(config-if)# exit
```

You can use these same queue-limit values in multiple output policy maps on the switch. However, changing one of the queue-limit values in a class would create a new, unique queue-limit configuration. You can attach only three unique queue-limit configurations in output policy maps to interfaces at any one time. If you try to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

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

You can 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.

remote-span

Use the **remote-span** VLAN configuration command to configure a VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN. Use the **no** form of this command to remove the RSPAN designation from the VLAN.

remote-span

no remote-span

- Syntax Description This command has no arguments or keywords.
- **Defaults** No RSPAN VLANs are defined.
- **Command Modes** VLAN configuration (config-VLAN)

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

Usage Guidelines Valid RSPAN VLAN IDs are 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).

Before you configure the RSPAN **remote-span** command, use the **vlan** global configuration command to create the VLAN.

- To change a VLAN from a user network interface (UNI) isolated VLAN (the default) to an RSPAN VLAN, enter the **rspan-vlan** VLAN configuration command.
- To change a UNI community VLAN to an RSPAN VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command.

The RSPAN VLAN has these characteristics:

- No MAC address learning occurs on it.
- RSPAN VLAN traffic flows only on trunk ports.
- Spanning Tree Protocol (STP) can run in the RSPAN VLAN, but it does not run on RSPAN destination ports. Note that only network node interfaces (NNIs) on the switch participate in STP.

You must manually also configure both source, destination, and intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch) with the RSPAN VLAN ID.

When an existing VLAN is configured as an RSPAN VLAN, the VLAN is first deleted and then recreated as an RSPAN VLAN. Any access ports become inactive until the RSPAN feature is disabled.

Examples This example shows how to configure a VLAN as an RSPAN VLAN. Switch(config)# vlan 901 Switch(config-vlan)# remote-span This example shows how to remove the RSPAN feature from a VLAN. Switch(config)# vlan 901 Switch(config-vlan)# no remote-span

You can verify your settings by entering the show vlan remote-span user EXEC command.

Commands Command Description monitor session Enables Switched Port Analyzer (SPAN) and RSPAN monitoring on a port and configures a port as a source or destination port. vlan Changes to config-vlan mode where you can configure VLANs 1 to 4094.

renew ip dhcp snooping database

Use the **renew ip dhcp snooping database** privileged EXEC command to renew the DHCP snooping binding database.

renew ip dhcp snooping database [validation none] [{flash:/filename |
ftp://user:password@host/filename | nvram:/filename | rcp://user@host/filename |
tftp://host/filename}] [validation none]

Syntax Description	validation none	(Optional) Specify that the switch does not verify the cyclic redundancy check (CRC) for the entries in the binding file specified by the URL.	
	flash:/filename	(Optional) Specify that the database agent or the binding file is in the flash memory.	
	ftp://user:password @host/filename	(Optional) Specify that the database agent or the binding file is on an FTP server.	
	nvram:/filename	(Optional) Specify that the database agent or the binding file is in the NVRAM.	
	rcp: //user@host/file name	(Optional) Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.	
	tftp://hostlfilename	(Optional) Specify that the database agent or the binding file is on a TFTP server.	
Defaults	No default is defined.		
Command Modes	Privileged EXEC		
Command History	Release Modification		
	12.2(25)EX This command was introduced.		
Usage Guidelines	If you do not specify a URL, the switch tries to read the file from the configured URL.		
Examples	This example shows how to renew the DHCP snooping binding database without checking CRC values:		
	Switch# renew ip dhcp snooping database validation none		
	You can verify settings by entering the show ip dhcp snooping database privileged EXEC command.		
Related Commands	Command	Description	
Related Commanus	ip dhcp snooping	Enables DHCP snooping on a VLAN.	
	ip dhcp snooping bin		
	show ip dhcp snooping bil		
	snow ip uncp snoopi	ing uatabase Displays the status of the DHCP shooping database agent.	