



Catalyst 3560 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 802.1x sessions. Use the **no** form of this command to disable 802.1x accounting.

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

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

Syntax Description

| | |
|-------------------|--|
| <i>name</i> | 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: <ul style="list-style-type: none"> <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. |
| radius | (Optional) Enable RADIUS authorization. |
| tacacs+ | (Optional) Enable TACACS+ accounting. |

■ **aaa accounting dot1x****Defaults**

AAA accounting is disabled.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

This command requires access to a RADIUS server.

**Note**

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring 802.1x RADIUS accounting on an interface.

Examples

This example shows how to configure 802.1x accounting:

```
Switch(config)# aaa accounting dot1x
Switch(config)#
```

**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 dot1x | Specifies one or more AAA methods for use on interfaces running 802.1x. |
| dot1x reauthentication | Sets the number of seconds between re-authentication attempts. |

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}
```

Syntax Description

| | |
|----------------|--|
| default | Use the listed authentication method that follows this argument as the default method when a user logs in. |
| <i>method1</i> | Enter the group radius keywords to use the list of all RADIUS servers for authentication. |



Note

Though other keywords are visible in the command-line help strings, only the **default** and **group radius** keywords are supported.

Defaults

No authentication is performed.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The *method* 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 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

Examples

This example shows how to enable AAA and how to create an 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 current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

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 action is to forward packets.

Command Modes

Access-map configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | 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 configuration mode, use the **match** access map configuration command to define the match conditions for a VLAN map. Use the **action** command to set the action that occurs when a packet matches the conditions.

The drop and forward parameters are not used in the **no** form of the command.

Examples

This example shows how to identify and apply a VLAN access map *vmap4* to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list *a12*:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address a12
Switch(config-access-map)# action forward
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 {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 | /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. |
| /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. |
| <i>source-url</i> | <p>The source URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> 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): rnp:[[/username@location]/directory]/image-name.tar The syntax for the TFTP: tftp:[[/location]/directory]/image-name.tar <p>The <i>image-name.tar</i> is the software image to download and install on the switch.</p> |

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.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-------------|---|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(20)SE | The http and https keywords were added. |

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 2-67.

Use the **/overwrite** option to overwrite the image on the flash device with the downloaded one.

If you specify the command *without* 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 *destination-url*
flash:/*file-url*

Create a new tar file on the local or network file system.

For *destination-url*, specify the 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 *tar-filename.tar* is the tar file to be created.

For **flash:**/*file-url*, specify the 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 <i>source-url</i> | <p>Display the contents of an existing tar file to the screen.</p> <p>For <i>source-url</i>, specify the source URL alias for the local or network file system. These options are supported:</p> <ul style="list-style-type: none"> • 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 <p>The <i>tar-filename.tar</i> is the tar file to display.</p> |
| /xtract <i>source-url</i> flash: <i>/file-url [dir/file...]</i> | <p>Extract files from a tar file to the local file system.</p> <p>For <i>source-url</i>, specify the source URL alias for the local file system. These options are supported:</p> <ul style="list-style-type: none"> • 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 <p>The <i>tar-filename.tar</i> is the tar file from which to extract.</p> <p>For flash:/file-url [dir/file...], specify the 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.</p> |

Defaults

None

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Filenames and directory names are case sensitive.

Image names are case sensitive.

Examples

This example shows how to create a tar file. The command writes the contents of the *new-configs* directory on the local flash device to a file named *saved.tar* 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 *c3560-tv0-m.tar* file that is in flash memory. The contents of the tar file appear on the screen:

```
Switch# archive tar /table flash:c3560-tv0-m.tar
info (219 bytes)
c3560-tv0-mz-121/ (directory)
c3560-tv0-mz-121/html/ (directory)
c3560-tv0-mz-121/html/foo.html (0 bytes)
c3560-tv0-mz-121/vegas-tv0-mz-121.bin (610856 bytes)
c3560-tv0-mz-121/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *c3560-tv0-mz-121/html* directory and its contents:

```
Switch# archive tar /table flash:c3560-tv0-m.tar c3560-tv0-mz-121/html
c3560-tv0-mz-121/html/ (directory)
c3560-tv0-mz-121/html/foo.html (0 bytes)
```

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 <i>version_string</i> | (Optional) Specify the specific version string of the image to be uploaded. |
| destination-url | <p>The destination URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> 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 <p>The <i>image-name.tar</i> is the name of software image to be stored on the server.</p> |

Defaults Uploads the currently running image from the flash: file system.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | 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 sensitive.

Examples This example shows how to upload the currently running image to a TFTP server at 172.20.140.2:

```
Switch# archive upload-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. |

arp access-list

Use the **arp access-list** global configuration command to define an Address Resolution Protocol (ARP) access control list (ACL) or to add clauses to the end of a previously defined list. Use the **no** form of this command to delete the specified ARP access list.

arp access-list *acl-name*

no arp access-list *acl-name*

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|-----------------|------------------|
| <i>acl-name</i> | Name of the ACL. |
|-----------------|------------------|

Defaults

No ARP access lists are defined.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

After entering the **arp access-list** command, you enter ARP access-list configuration mode, and these configuration commands are available:

- **default:** returns a command to its default setting.
- **deny:** specifies packets to reject. For more information, see the “[deny \(ARP access-list configuration\)](#)” section on page 2-68.
- **exit:** exits ARP access-list configuration mode.
- **no:** negates a command or returns to default settings.
- **permit:** specifies packets to forward. For more information, see the “[permit \(ARP access-list configuration\)](#)” section on page 2-244.

Use the **permit** and **deny** access-list configuration commands to forward and to drop ARP packets based on the specified matching criteria.

When the ARP ACL is defined, you can apply it to a VLAN by using the **ip arp inspection filter vlan** global configuration command. ARP packets containing only IP-to-MAC address bindings are compared to the ACL. All other types of packets are bridged in the ingress VLAN without validation. If the ACL permits a packet, the switch forwards it. If the ACL denies a packet because of an explicit deny statement, the switch drops the packet. If the ACL denies a packet because of an implicit deny statement, the switch compares the packet to the list of DHCP bindings (unless the ACL is *static*, which means that packets are not compared to the bindings).

Examples

This example shows how to define an ARP access list and to permit both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 00001.0000.abcd
Switch(config-arp-nacl)# end
```

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

Related Commands

| Command | Description |
|---|---|
| deny (ARP access-list configuration) | Denies an ARP packet based on matches compared against the DHCP bindings. |
| ip arp inspection filter vlan | Permits ARP requests and responses from a host configured with a static IP address. |
| permit (ARP access-list configuration) | Permits an ARP packet based on matches compared against the DHCP bindings. |
| show arp access-list | Displays detailed information about ARP access lists. |

auto qos voip

Use the **auto qos voip** interface configuration command to automatically configure quality of service (QoS) for voice over IP (VoIP) within a QoS domain. Use the **no** form of this command to return to the default setting.

auto qos voip { **cisco-phone** | **cisco-softphone** | **trust** }

no auto qos voip [**cisco-phone** | **cisco-softphone** | **trust**]

Syntax Description

| | |
|------------------------|--|
| cisco-phone | Identify this port as connected to a Cisco IP Phone, and automatically configure QoS for VoIP. The QoS labels of incoming packets are trusted only when the telephone is detected. |
| cisco-softphone | Identify this port as connected to a device running the Cisco SoftPhone, and automatically configure QoS for VoIP. |
| trust | Identify this port as connected to a trusted switch or router, and automatically configure QoS for VoIP. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted. |

Defaults

Auto-QoS is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues as shown in [Table 2-1](#).

Table 2-1 Traffic Types, Packet Labels, and Queues

| | VoIP Data Traffic | VoIP Control Traffic | Routing Protocol Traffic | STP ¹ BPDU ² Traffic | Real-Time Video Traffic | All Other Traffic | |
|--------------------------|----------------------------|----------------------|--------------------------|--|-------------------------|-------------------|----------------|
| DSCP ³ | 46 | 24, 26 | 48 | 56 | 34 | – | |
| CoS ⁴ | 5 | 3 | 6 | 7 | 3 | – | |
| CoS-to-Ingress Queue Map | 2, 3, 4, 5, 6, 7 (queue 2) | | | | | 0, 1 (queue 1) | |
| CoS-to-Egress Queue Map | 5 (queue 1) | 3, 6, 7 (queue 2) | | | 4 (queue 3) | 2 (queue 3) | 0, 1 (queue 4) |

1. STP = Spanning Tree Protocol
2. BPDU = bridge protocol data unit
3. DSCP = Differentiated Services Code Point
4. CoS = class of service

Table 2-2 shows the generated auto-QoS configuration for the ingress queues.

Table 2-2 Auto-QoS Configuration for the Ingress Queues

| Ingress Queue | Queue Number | CoS-to-Queue Map | Queue Weight (Bandwidth) | Queue (Buffer) Size |
|-------------------------|--------------|------------------|--------------------------|---------------------|
| SRR ¹ shared | 1 | 0, 1 | 81 percent | 67 percent |
| Priority | 2 | 2, 3, 4, 5, 6, 7 | 19 percent | 33 percent |

1. SRR = shaped round robin. Ingress queues support shared mode only.

Table 2-3 shows the generated auto-QoS configuration for the egress queues.

Table 2-3 Auto-QoS Configuration for the Egress Queues

| Egress Queue | Queue Number | CoS-to-Queue Map | Queue Weight (Bandwidth) | Queue (Buffer) Size for Gigabit-Capable Ports | Queue (Buffer) Size for 10/100 Ethernet Ports |
|-------------------|--------------|------------------|--------------------------|---|---|
| Priority (shaped) | 1 | 5 | 10 percent | 16 percent | 10 percent |
| SRR shared | 2 | 3, 6, 7 | 10 percent | 6 percent | 10 percent |
| SRR shared | 3 | 2, 4 | 60 percent | 17 percent | 26 percent |
| SRR shared | 4 | 0, 1 | 20 percent | 61 percent | 54 percent |

Command Modes Interface configuration

Command History

| Release | Modification |
|-------------|---|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(20)SE | The cisco-softphone keyword was added, and the generated auto-QoS configuration changed. |

Usage Guidelines

Use this command to configure the QoS appropriate for VoIP traffic within the QoS domain. The QoS domain includes the switch, the interior of the network, and edge devices that can classify incoming traffic for QoS.

In releases earlier than Cisco IOS Release 12.2(20)SE, auto-QoS configures the switch only for VoIP with Cisco IP Phones on switch ports.

In Cisco IOS Release 12.2(20)SE or later, auto-QoS configures the switch for VoIP with Cisco IP Phones on switch and routed ports and for VoIP with devices running the Cisco SoftPhone application. These releases support only Cisco IP SoftPhone Version 1.3(3) or later. Connected devices must use Cisco Call Manager Version 4 or later.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

**Note**

The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.
- When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP Phone, the switch enables the trusted boundary feature. The switch uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP Phone. When a Cisco IP Phone is detected, the ingress classification on the port is set to trust the QoS label received in the packet. When a Cisco IP Phone is absent, the ingress classification is set to not trust the QoS label in the packet. The switch configures ingress and egress queues on the port according to the settings in [Table 2-2](#) and [Table 2-3](#).
- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the switch uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. The switch configures ingress and egress queues on the port according to the settings in [Table 2-2](#) and [Table 2-3](#).
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the interior of the network, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices). The switch configures the ingress and egress queues on the port according to the settings in [Table 2-2](#) and [Table 2-3](#).

You can enable auto-QoS on static, dynamic-access, and voice VLAN access, and trunk ports. When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.

**Note**

When a device running Cisco SoftPhone is connected to a switch or routed port, the switch supports only one Cisco SoftPhone application per port.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging. For more information, see the **debug auto qos** command.

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

Examples

This example shows how to enable auto-QoS and to trust the QoS labels received in incoming packets when the switch or router connected to the port is a trusted device:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip trust
```

You can verify your settings by entering the **show auto qos interface interface-id** privileged EXEC command.

Related Commands

| Command | Description |
|---|---|
| debug auto qos | Enables debugging of the auto-QoS feature. |
| mls qos cos | Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port. |
| mls qos map { cos-dscp <i>dscp1 ... dscp8</i> dscp-cos <i>dscp-list to cos</i> } | Defines the CoS-to-DSCP map or the DSCP-to-CoS map. |
| mls qos queue-set output buffers | Allocates buffers to a queue-set. |
| mls qos srr-queue input bandwidth | Assigns shaped round robin (SRR) weights to an ingress queue. |
| mls qos srr-queue input buffers | Allocates the buffers between the ingress queues. |
| mls qos srr-queue input cos-map | Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID. |
| mls qos srr-queue input dscp-map | Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID. |
| mls qos srr-queue input priority-queue | Configures the ingress priority queue and guarantees bandwidth. |
| mls qos srr-queue output cos-map | Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID. |
| mls qos srr-queue output dscp-map | Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID. |
| mls qos trust | Configures the port trust state. |
| queue-set | Maps a port to a queue-set. |
| show auto qos | Displays auto-QoS information. |
| show mls qos interface | Displays QoS information at the port level. |

| Command | Description |
|---|--|
| srr-queue bandwidth shape | Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port. |
| srr-queue bandwidth share | Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port. |

boot bootlpr

Use the **boot bootlpr** 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 bootlpr filesystem:/file-url
```

```
no boot bootlpr
```

| Syntax Description | | |
|--------------------|--------------------|---|
| | <i>filesystem:</i> | Alias for a flash file system. Use flash: for the system board flash device. |
| | <i>/file-url</i> | The path (directory) and name of a bootable helper image. |

| Defaults | |
|----------|----------------------------|
| | No helper image is loaded. |

| Command Modes | |
|---------------|----------------------|
| | Global configuration |

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

| Usage Guidelines | |
|------------------|--|
| | Filenames and directory names are case sensitive. |
| | This command changes the setting of the BOOTHLPR environment variable. For more information, see Appendix A, “Catalyst 3560 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: <i>/file-url</i> | The path (directory) and name of the configuration file. |
|--------------------------------|--|

Defaults

The default configuration file is flash:config.text.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the CONFIG_FILE environment variable. For more information, see [Appendix A, “Catalyst 3560 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

Syntax Description

This command has no arguments or keywords.

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 |
|-------------|------------------------------|
| 12.1(19)EA1 | 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.



Note

Despite the setting of this command, you can interrupt the automatic boot process at any time by pressing the MODE button on the switch front panel.

This command changes the setting of the ENABLE_BREAK environment variable. For more information, see [Appendix A, “Catalyst 3560 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

| | |
|--------------------|--|
| <i>filesystem:</i> | Alias for a flash file system. Use flash: for the system board flash device. |
| <i>/file-url</i> | 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 loaded.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER environment variable. For more information, see [Appendix A, “Catalyst 3560 Switch Boot Loader Commands.”](#)

Related Commands

| Command | Description |
|---------------------------|--|
| show boot | Displays the settings of the boot environment variables. |

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 | | |
|--------------------|--------------------|---|
| | <i>filesystem:</i> | Alias for a flash file system. Use flash: for the system board flash device. |
| | <i>/file-url</i> | The path (directory) and helper configuration file to load. |

Defaults No helper configuration file is specified.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines This variable is used only for internal development and testing.
 Filenames and directory names are case sensitive.
 This command changes the setting of the HELPER_CONFIG_FILE environment variable. For more information, see [Appendix A, “Catalyst 3560 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 |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | 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, “Catalyst 3560 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 | <i>filename</i> | The name of the private configuration file. |
|--------------------|-----------------|---|
|--------------------|-----------------|---|

| Defaults | The default configuration file is <i>private-config</i> . |
|----------|---|
|----------|---|

| Command Modes | Global configuration |
|---------------|----------------------|
|---------------|----------------------|

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

| Usage Guidelines | Filenames are case sensitive. |
|------------------|-------------------------------|
|------------------|-------------------------------|

| Examples | This example shows how to specify the name of the private configuration file to be <i>pconfig</i> : |
|----------|---|
|----------|---|

```
Switch(config)# boot 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

| Syntax Description | | |
|--------------------|--------------------|---|
| | <i>filesystem:</i> | Alias for a flash file system. Use flash: for the system board flash device. |
| | <i>/file-url</i> | 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 it 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 the original directory. |

| Command Modes | |
|---------------|----------------------|
| | Global configuration |

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

| Usage Guidelines | |
|------------------|---|
| | <p>Filenames and directory names are case sensitive.</p> <p>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.</p> <p>This command changes the setting of the BOOT environment variable. For more information, see Appendix A, “Catalyst 3560 Switch Boot Loader Commands.”</p> |

| Related Commands | Command | Description |
|------------------|---------------------------|--|
| | 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
```

Syntax Description

| | |
|-----------------------------|---|
| <i>channel-group-number</i> | Specify the channel group number. The range is 1 to 48. |
| mode | Specify the EtherChannel mode. |
| active | Unconditionally enable Link Aggregation Control Protocol (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 Port Aggregation Protocol (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) Used with the auto or desirable keyword when traffic is expected from the other device. |
| on | Force the port to channel without PAgP or the LACP. With the on mode, a usable EtherChannel exists only when a port group in the on mode is connected to another port group 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 configured.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|--|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(25)SE | The <i>channel-group-number</i> range was changed from 1 to 12 to 1 to 48. |

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first by using the **interface port-channel** global configuration command before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port if the logical interface is not already created. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

You do not have to disable the IP address that is assigned to a physical port that is part of a channel group, but we strongly recommend that you do so.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. You should manually configure the port-channel logical interface before putting the interface into the channel group.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

If you do not specify **non-silent** with the **auto** or **desirable** mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. A example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

**Caution**

With the **on** mode, a usable EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode. 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.

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 802.1x port. If you try to enable 802.1x on an EtherChannel port, an error message appears, and 802.1x is not enabled.

**Note**

If 802.1x is enabled on a not-yet active port of an EtherChannel in software releases earlier than Cisco IOS Release 12.2(18)SE, the port does not join the EtherChannel.

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.

**Caution**

Do not enable Layer 3 addresses on the physical EtherChannel ports. Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

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

| 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 current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

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 configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

Examples

This example shows how to specify LACP as the protocol that manages the EtherChannel:

```
Switch(config-if)# channel-protocol lacp
```

You can verify your settings by entering the **show etherchannel [channel-group-number] protocol** privileged EXEC 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 define a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name. Use the **no** form of this command to delete an existing class map.

```
class class-map-name
```

```
no class class-map-name
```

Syntax Description

| | |
|-----------------------|------------------------|
| <i>class-map-name</i> | Name of the class map. |
|-----------------------|------------------------|

Defaults

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter policy-map class configuration mode, and these configuration commands are available:

- **exit**: exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**: returns a command to its default setting.
- **police**: defines a 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 commands.
- **set**: specifies a value to be assigned to the classified traffic. For more information, see the **set** command.
- **trust**: defines a trust state for traffic classified with the **class** or the **class-map** command. For more information, see the **trust** command.

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

The **class** command performs the same function as the **class-map global configuration command**. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

Examples

This example shows how to create a policy map called *policy1*. When attached to the ingress direction, it matches all the incoming traffic defined in *class1*, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mbps and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
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. |
| 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. |
| set | Classifies IP traffic by setting a DSCP or IP-precedence value in the packet. |
| show policy-map | Displays quality of service (QoS) policy maps. |
| trust | Defines a trust state for the traffic classified through the class policy-map configuration command or the class-map global configuration command. |

class-map

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

```
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. All criteria in the class map must be matched. |
| match-any | (Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched. |
| <i>class-map-name</i> | Name of the class map. |

Defaults

No class maps are defined.

If neither the **match-all** or **match-any** keyword is specified, the default is **match-all**.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) 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 from QoS class-map configuration mode.
- **match:** configures classification criteria. For more information, see the [match \(class-map configuration\)](#) command.
- **no:** removes a match statement from a class map.
- **rename:** renames the current class map. If you rename a class map with a name that is already used, the message `A class-map with this name already exists` appears.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-all** and **match-any** keywords are equivalent.

Only one access control list (ACL) can be configured in a class map. The ACL can have multiple access control entries (ACEs).

Examples

This example shows how to configure the class map called *class1* with one match criterion, which is an access list called *103*:

```
Switch(config)# access-list 103 permit any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

This example shows how to delete the class map *class1*:

```
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 (through the police , set , and trust policy-map class configuration commands) for the specified class-map name. |
| match (class-map configuration) | Defines the match criteria to classify traffic. |
| 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 arp inspection log

Use the **clear ip arp inspection log** privileged EXEC command to clear the dynamic Address Resolution Protocol (ARP) inspection log buffer.

clear ip arp inspection log

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Examples

This example shows how to clear the contents of the log buffer:

```
Switch# clear ip arp inspection log
```

You can verify that the log was cleared by entering the **show ip arp inspection log** privileged command.

Related Commands

| Command | Description |
|--|---|
| arp access-list | Defines an ARP access control list (ACL). |
| ip arp inspection log-buffer | Configures the dynamic ARP inspection logging buffer. |
| ip arp inspection vlan logging | Controls the type of packets that are logged per VLAN. |
| show ip arp inspection log | Displays the configuration and contents of the dynamic ARP inspection log buffer. |

clear ip arp inspection statistics

Use the **clear ip arp inspection statistics** privileged EXEC command to clear the dynamic Address Resolution Protocol (ARP) inspection statistics.

clear ip arp inspection statistics [*vlan vlan-range*]

This command is available only if your switch is running the enhanced multilayer image (EMI).

| | | |
|---------------------------|--|--|
| Syntax Description | vlan <i>vlan-range</i> | (Optional) Clear statistics for the specified VLAN or VLANs. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| Defaults | No default is defined. | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | 12.2(20)SE | This command was introduced. |
| Examples | <p>This example shows how to clear the statistics for VLAN 1:</p> <pre>Switch# clear ip arp inspection statistics vlan 1</pre> <p>You can verify that the statistics were deleted by entering the show ip arp inspection statistics vlan 1 privileged EXEC command.</p> | |
| Related Commands | Command | Description |
| | show ip arp inspection statistics | Displays statistics for forwarded, dropped, MAC validation failure, and IP validation failure packets for all VLANs or the specified VLAN. |

clear ip dhcp snooping database

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

clear ip dhcp snooping database statistics

This command is available only if your switch is running the enhanced multilayer image (EMI).

| | |
|---------------------------|--|
| Syntax Description | statistics Clear the DHCP snooping binding database agent statistics. |
|---------------------------|--|

| | |
|-----------------|------------------------|
| Defaults | No default is defined. |
|-----------------|------------------------|

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

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.2(20)SE | This command 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.

| Related Commands | Command | Description |
|-------------------------|---|--|
| | ip dhcp snooping | Enables DHCP snooping on a VLAN. |
| | ip dhcp snooping database | Configures the DHCP snooping binding database agent or the binding file. |
| | show ip dhcp snooping binding | Displays the status of DHCP snooping database agent. |

clear ipc

Use the **clear ipc** privileged EXEC command on the switch stack or on a standalone switch to clear Interprocess Communications Protocol (IPC) statistics.

```
clear ipc {queue-statistics | statistics}
```

| Syntax Description | queue-statistics | Clear the IPC queue statistics. |
|--------------------|------------------|---------------------------------|
| | statistics | Clear the IPC statistics. |

Defaults No default is defined.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|------------------------------|
| | 12.2(20)SE | This command was introduced. |

Usage Guidelines You can clear all statistics by using the **clear ipc statistics** command, or you can clear only the queue statistics by using the **clear ipc queue-statistics** command.

Examples This example shows how to clear all statistics:

```
Switch# clear ipc statistics
```

This example shows how to clear only the queue statistics:

```
Switch# clear ipc queue-statistics
```

You can verify that the statistics were deleted by entering the **show ipc rpc** or the **show ipc session** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|--|--|
| | show ipc {rpc session} | Displays the IPC multicast routing statistics. |

clear l2protocol-tunnel counters

Use the **clear l2protocol-tunnel counters** privileged EXEC command to clear the protocol counters in protocol tunnel ports.

clear l2protocol-tunnel counters [*interface-id*]

| | | |
|---------------------------|---------------------|--|
| Syntax Description | <i>interface-id</i> | (Optional) Specify interface (physical interface or port channel) for which protocol counters are to be cleared. |
|---------------------------|---------------------|--|

| | |
|-----------------|-------------------------------|
| Defaults | This command has no defaults. |
|-----------------|-------------------------------|

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

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.2(25)SE | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | Use this command to clear protocol tunnel counters on the switch or on the specified interface. |
|-------------------------|---|

Examples This example shows how to clear Layer 2 protocol tunnel counters on an interface:

```
Switch# clear l2protocol-tunnel counters gigabitethernet0/3
```

| Related Commands | Command | Description |
|-------------------------|--|---|
| | show l2protocol-tunnel | Displays information about ports configured for Layer 2 protocol tunneling. |

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}
```

| Syntax Description | |
|-----------------------------|--|
| <i>channel-group-number</i> | (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 |
|-----------------|-------------|--|
| | 12.1(19)EA1 | This command was introduced. |
| | 12.2(25)SE | The <i>channel-group-number</i> range was changed from 1 to 12 to 1 to 48. |

Usage Guidelines You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp *channel-group-number* counters** command.

Examples This example shows how to clear all channel-group information:

```
Switch# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:

```
Switch# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp 4 counters** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|---------------------------|--|
| | show lacp | Displays LACP channel-group information. |

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 dynamic MAC addresses. |
| dynamic address <i>mac-addr</i> | | (Optional) Delete the specified dynamic MAC address. |
| dynamic interface <i>interface-id</i> | | (Optional) Delete all dynamic MAC addresses on the specified physical port or port channel. |
| dynamic vlan <i>vlan-id</i> | | (Optional) Delete all dynamic MAC addresses for the specified VLAN. The range is 1 to 4096. |
| notification | | Clear the notifications in the history table and reset the counters. |

Defaults No default is defined.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command 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 information was deleted by entering the **show mac address-table** privileged EXEC command.

■ clear mac address-table

| Related Commands | Command | Description |
|------------------|---|--|
| | mac address-table notification | Enables the MAC address notification feature. |
| | show mac address-table | Displays the MAC address table static and dynamic entries. |
| | show mac address-table notification | Displays the MAC address notification settings for all interfaces or the specified interface. |
| | snmp trap mac-notification | Enables the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific 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}
```

Syntax Description

| | |
|-----------------------------|--|
| <i>channel-group-number</i> | (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 |
|-------------|--|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(25)SE | The <i>channel-group-number</i> range was changed from 1 to 12 to 1 to 48. |

Usage Guidelines

You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp channel-group-number counters** command.

Examples

This example shows how to clear all channel-group information:

```
Switch# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Switch# clear pagp 10 counters
```

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

Related Commands

| Command | Description |
|---------------------------|--|
| show pagp | Displays PAgP channel-group information. |

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]]
```

| 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 <i>mac-addr</i> | (Optional) | Delete the specified dynamic secure MAC address. |
| interface <i>interface-id</i> | (Optional) | Delete all the dynamic secure MAC addresses on the specified physical port or VLAN. |
| vlan <i>vlan-id</i> | (Optional) | VLAN ID of the VLAN on which this address should be cleared. |

Defaults No default is defined.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.2(25)SEA | This command was introduced. |

Examples This example shows how 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:

```
Switch# clear port-security dynamic interface gigabitethernet0/1
```

This example shows how to remove all the dynamic secure addresses from the address table:

```
Switch# clear port-security dynamic
```

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 <i>mac-address</i> | 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 <i>interface-id</i> (Optional) Clear all spanning-tree counters on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48. | | | | |
|------------------------------------|---|---------|--------------|------------------------------------|---|
| Defaults | No default is defined. | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(19)EA1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | 12.1(19)EA1 | This command was introduced. |
| Release | Modification | | | | |
| 12.1(19)EA1 | This command was introduced. | | | | |
| Usage Guidelines | If the <i>interface-id</i> is not specified, spanning-tree counters are cleared for all interfaces. | | | | |
| Examples | <p>This example shows how to clear spanning-tree counters for all interfaces:</p> <pre>Switch# clear spanning-tree counters</pre> | | | | |
| Related Commands | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show spanning-tree</td> <td>Displays spanning-tree state information.</td> </tr> </tbody> </table> | Command | Description | show spanning-tree | Displays spanning-tree state information. |
| 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 interfaces or on the specified interface.

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

| | |
|---------------------------|---|
| Syntax Description | interface <i>interface-id</i> (Optional) Restart the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48. |
|---------------------------|---|

| | |
|-----------------|------------------------|
| Defaults | No default is defined. |
|-----------------|------------------------|

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

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

A switch running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If a rapid-PVST+ switch or an MSTP switch receives a legacy 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, it sends only 802.1D BPDUs on that port. A multiple spanning-tree (MST) switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

However, the switch does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives 802.1D BPDUs because it cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

Examples

This example shows how to restart the protocol migration process on a port:

```
Switch# clear spanning-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 arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Examples This example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Switch# clear vmps statistics
```

You can verify that information was deleted by entering the **show vmps statistics** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|---------------------------|---|
| | show vmps | Displays the VQP version, reconfirmation interval, retry count, VMPS IP addresses, and the current and primary servers. |

clear vtp counters

Use the **clear vtp counters** privileged EXEC command to clear the VLAN Trunking Protocol (VTP) and pruning counters.

clear vtp counters

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Examples This example shows how to clear the VTP counters:

```
Switch# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|--------------------------|---|
| | show vtp | Displays general information about the VTP management domain, status, and counters. |

cluster commander-address

You do not need to enter this command. The cluster command switch automatically provides its MAC address to cluster member switches when these switches join the cluster. The cluster member switch adds this information and other cluster information to its running configuration file. Use the **no** form of this global configuration command from the cluster member switch console port to remove the switch from a cluster only during debugging or recovery procedures.

cluster commander-address *mac-address* [**member number name name**]

no cluster commander-address

| Syntax Description | | |
|--------------------|----------------------|--|
| | <i>mac-address</i> | MAC address of the cluster command switch. |
| | member number | (Optional) Number of a configured cluster member switch. The range is 0 to 15. |
| | name name | (Optional) Name of the configured cluster up to 31 characters. |

Defaults The switch is not a member of any cluster.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines This command is available only on the cluster command switch.

A cluster member can have only one cluster command switch.

The cluster member switch retains the identity of the cluster command switch during a system reload by using the *mac-address* parameter.

You can enter the **no** form on a cluster member switch to remove it from the cluster during debugging or recovery procedures. You would normally use this command from the cluster member switch console port only when the member has lost communication with the cluster command switch. With normal switch configuration, we recommend that you remove cluster member switches only by entering the **no cluster member n** global configuration command on the cluster command switch.

When a standby cluster command switch becomes active (becomes the cluster command switch), it removes the cluster commander address line from its configuration.

Examples

This is partial sample output from the running configuration of a cluster member.

```
Switch(config)# show running-configuration
```

```
<output truncated>
```

```
cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster
```

```
<output truncated>
```

This example shows how to remove a member from the cluster by using the cluster member console.

```
Switch # configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)# no cluster commander-address
```

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

Related Commands

| Command | Description |
|------------------------------|---|
| show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. |

cluster discovery hop-count

Use the **cluster discovery hop-count** global configuration command on the cluster command switch to set the hop-count limit for extended discovery of candidate switches. Use the **no** form of this command to return to the default setting.

cluster discovery hop-count *number*

no cluster discovery hop-count

| | | |
|---------------------------|---------------|---|
| Syntax Description | <i>number</i> | Number of hops from the cluster edge that the cluster command switch limits the discovery of candidates. The range is 1 to 7. |
|---------------------------|---------------|---|

Defaults The hop count is set to 3.

Command Modes Global configuration

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines This command is available only on the cluster command switch. This command does not operate on cluster member switches.

If the hop count is set to 1, it disables extended discovery. The cluster command switch discovers only candidates that are one hop from the edge of the cluster. The edge of the cluster is the point between the last discovered cluster member switch and the first discovered candidate switch.

Examples This example shows how to set hop count limit to 4. This command is executed on the cluster command switch.

```
Switch(config)# cluster discovery hop-count 4
```

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

| Related Commands | Command | Description |
|-------------------------|---|---|
| | show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. |
| | show cluster candidates | Displays a list of candidate switches. |

cluster enable

Use the **cluster enable** global configuration command on a command-capable switch to enable it as the cluster command switch, assign a cluster name, and to optionally assign a member number to it. Use the **no** form of the command to remove all members and to make the cluster command switch a candidate switch.

cluster enable *name* [*command-switch-member-number*]

no cluster enable

| Syntax Description | | |
|-------------------------------------|--|--|
| <i>name</i> | Name of the cluster up to 31 characters. Valid characters include only alphanumerics, dashes, and underscores. | |
| <i>command-switch-member-number</i> | (Optional) Assign a member number to the cluster command switch of the cluster. The range is 0 to 15. | |

Defaults

The switch is not a cluster command switch.

No cluster name is defined.

The member number is 0 when the switch is the cluster command switch.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Enter this command on any command-capable switch that is not part of any cluster. This command fails if a device is already configured as a member of the cluster.

You must name the cluster when you enable the cluster command switch. If the switch is already configured as the cluster command switch, this command changes the cluster name if it is different from the previous cluster name.

Examples

This example shows how to enable the cluster command switch, name the cluster, and set the cluster command switch member number to 4.

```
Switch(config)# cluster enable Engineering-IDF4 4
```

You can verify your setting by entering the **show cluster** privileged EXEC command on the cluster command switch.

cluster enable

| Related Commands | Command | Description |
|------------------|------------------------------|---|
| | show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. |

cluster holdtime

Use the **cluster holdtime** global configuration command to set the duration in seconds before a switch (either the command or cluster member switch) declares the other switch down after not receiving heartbeat messages. Use the **no** form of this command to set the duration to the default value.

cluster holdtime *holdtime-in-secs*

no cluster holdtime

| Syntax Description | <i>holdtime-in-secs</i> | Duration in seconds before a switch (either a command or cluster member switch) declares the other switch down. The range is 1 to 300 seconds. | | | | |
|------------------------------|--|--|--------------|------------------------------|---|--|
| Defaults | The default holdtime is 80 seconds. | | | | | |
| Command Modes | Global configuration | | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(19)EA1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | 12.1(19)EA1 | This command was introduced. | |
| Release | Modification | | | | | |
| 12.1(19)EA1 | This command was introduced. | | | | | |
| Usage Guidelines | <p>Enter this command with the cluster timer global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.</p> <p>The holdtime is typically set as a multiple of the interval timer (cluster timer). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.</p> | | | | | |
| Examples | <p>This example shows how to change the interval timer and the duration on the cluster command switch.</p> <pre>Switch(config)# cluster timer 3 Switch(config)# cluster holdtime 30</pre> <p>You can verify your settings by entering the show cluster privileged EXEC command.</p> | | | | | |
| Related Commands | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show cluster</td> <td>Displays the cluster status and a summary of the cluster to which the switch belongs.</td> </tr> </tbody> </table> | Command | Description | show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. | |
| Command | Description | | | | | |
| show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. | | | | | |

cluster member

Use the **cluster member** global configuration command on the cluster command switch to add candidates to a cluster. Use the **no** form of the command to remove members from the cluster.

cluster member [*n*] **mac-address** *H.H.H* [**password** *enable-password*] [**vlan** *vlan-id*]

no cluster member *n*

Syntax Description

| | |
|--|---|
| <i>n</i> | The number that identifies a cluster member. The range is 0 to 15. |
| mac-address <i>H.H.H</i> | MAC address of the cluster member switch in hexadecimal format. |
| password <i>enable-password</i> | Enable password of the candidate switch. The password is not required if there is no password on the candidate switch. |
| vlan <i>vlan-id</i> | (Optional) VLAN ID through which the candidate is added to the cluster by the cluster command switch. The range is 1 to 4094. |

Defaults

A newly enabled cluster command switch has no associated cluster members.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Enter this command only on the cluster command switch to add a candidate to or remove a member from the cluster. If you enter this command on a switch other than the cluster command switch, the switch rejects the command and displays an error message.

You must enter a member number to remove a switch from the cluster. However, you do not need to enter a member number to add a switch to the cluster. The cluster command switch selects the next available member number and assigns it to the switch that is joining the cluster.

You must enter the enable password of the candidate switch for authentication when it joins the cluster. The password is not saved in the running or startup configuration. After a candidate switch becomes a member of the cluster, its password becomes the same as the cluster command-switch password.

If a switch does not have a configured hostname, the cluster command switch appends a member number to the cluster command-switch hostname and assigns it to the cluster member switch.

If you do not specify a VLAN ID, the cluster command switch automatically chooses a VLAN and adds the candidate to the cluster.

Examples

This example shows how to add a switch as member 2 with MAC address 00E0.1E00.2222 and the password *key* to a cluster. The cluster command switch adds the candidate to the cluster through VLAN 3.

```
Switch(config)# cluster member 2 mac-address 00E0.1E00.2222 password key vlan 3
```

This example shows how to add a switch with MAC address 00E0.1E00.3333 to the cluster. This switch does not have a password. The cluster command switch selects the next available member number and assigns it to the switch that is joining the cluster.

```
Switch(config)# cluster member mac-address 00E0.1E00.3333
```

You can verify your settings by entering the **show cluster members** privileged EXEC command on the cluster command switch.

Related Commands

| Command | Description |
|---|---|
| show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. |
| show cluster candidates | Displays a list of candidate switches. |
| show cluster members | Displays information about the cluster members. |

cluster outside-interface

Use the **cluster outside-interface** global configuration command to configure the outside interface for cluster Network Address Translation (NAT) so that a member without an IP address can communicate with devices outside the cluster. Use the **no** form of this command to return to the default setting.

cluster outside-interface *interface-id*

no cluster outside-interface

| | | |
|---------------------------|---------------------|---|
| Syntax Description | <i>interface-id</i> | Interface to serve as the outside interface. Valid interfaces include physical interfaces, port-channels, or VLANs. The port-channel range is 1 to 48. The VLAN range is 1 to 4094. |
|---------------------------|---------------------|---|

Defaults The default outside interface is automatically selected by the cluster command switch.

Command Modes Global configuration

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines Enter this command only on the cluster command switch. If you enter this command on a cluster member switch, an error message appears.

Examples This example shows how to set the outside interface to VLAN 1:

```
Switch(config)# cluster outside-interface vlan 1
```

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

| Related Commands | Command | Description |
|-------------------------|----------------------------|--|
| | show running-config | Displays the current operating configuration. For syntax information, select the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

cluster run

Use the **cluster run** global configuration command to enable clustering on a switch. Use the **no** form of this command to disable clustering on a switch.

cluster run

no cluster run

Syntax Description This command has no arguments or keywords.

Defaults Clustering is enabled on all switches.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines When you enter the **no cluster run** command on a cluster command switch, the cluster command switch is disabled. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a cluster member switch, it is removed from the cluster. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a switch that is not part of a cluster, clustering is disabled on this switch. This switch cannot then become a candidate switch.

Examples This example shows how to disable clustering on the cluster command switch:

```
Switch(config)# no cluster run
```

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

| Related Commands | Command | Description |
|------------------|------------------------------|---|
| | show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. |

cluster standby-group

Use the **cluster standby-group** global configuration command to enable cluster command-switch redundancy by binding the cluster to an existing Hot Standby Router Protocol (HSRP). Entering the **routing-redundancy** keyword enables the same HSRP group to be used for cluster command-switch redundancy and routing redundancy. Use the **no** form of this command to return to the default setting.

cluster standby-group *HSRP-group-name* [**routing-redundancy**]

no cluster standby-group

Syntax Description

| | |
|---------------------------|--|
| <i>HSRP-group-name</i> | Name of the HSRP group that is bound to the cluster. The group name is limited to 32 characters. |
| routing-redundancy | (Optional) Enable the same HSRP standby group to be used for cluster command-switch redundancy and routing redundancy. |

Defaults

The cluster is not bound to any HSRP group.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Enter this command only on the cluster command switch. If you enter it on a cluster member switch, an error message appears.

The cluster command switch propagates the cluster-HSRP binding information to all cluster-HSRP capable members. Each cluster member switch stores the binding information in its NVRAM. The HSRP group name must be a valid standby group; otherwise, the command exits with an error.

The same group name should be used on all members of the HSRP standby group that is to be bound to the cluster. The same HSRP group name should also be used on all cluster-HSRP capable members for the HSRP group that is to be bound. (When not binding a cluster to an HSRP group, you can use different names on the cluster commander and the members.)

Examples

This example shows how to bind the HSRP group named *my_hsrp* to the cluster. This command is executed on the cluster command switch.

```
Switch(config)# cluster standby-group my_hsrp
```

This example shows how to use the same HSRP group named *my_hsrp* for routing redundancy and cluster redundancy.

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
```

This example shows the error message when this command is executed on a cluster command switch and the specified HSRP standby group does not exist:

```
Switch(config)# cluster standby-group my_hsrp
%ERROR: Standby (my_hsrp) group does not exist
```

This example shows the error message when this command is executed on a cluster member switch:

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
%ERROR: This command runs on a cluster command switch
```

You can verify your settings by entering the **show cluster** privileged EXEC command. The output shows whether redundancy is enabled in the cluster.

Related Commands

| Command | Description |
|---------------------|---|
| standby ip | Enables HSRP on the interface. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands . |
| show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. |
| show standby | Displays standby group information. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands . |

cluster timer

Use the **cluster timer** global configuration command to set the interval in seconds between heartbeat messages. Use the **no** form of this command to set the interval to the default value.

cluster timer *interval-in-secs*

no cluster timer

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | <i>interval-in-secs</i> | Interval in seconds between heartbeat messages. The range is 1 to 300 seconds. |
|---------------------------|-------------------------|--|

| | |
|-----------------|----------------------------|
| Defaults | The interval is 8 seconds. |
|-----------------|----------------------------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines Enter this command with the **cluster holdtime** global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the heartbeat interval timer (**cluster timer**). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

Examples This example shows how to change the heartbeat interval timer and the duration on the cluster command switch:

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

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

| | | |
|-------------------------|------------------------------|---|
| Related Commands | Command | Description |
| | show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. |

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 | |
|------------------------|---|
| <i>macro-name</i> | Name of the interface-range macro; up to 32 characters. |
| <i>interface-range</i> | Interface range; for valid values for interface ranges, see “Usage Guidelines.” |

Defaults This command has no default setting.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | 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 *interface-range*, use this format:

- *type {first-interface} - {last-interface}*
- You must add a space between the first interface number and the hyphen when entering an *interface-range*. For example, **gigabitethernet 0/1 - 2** is a valid range; **gigabitethernet 0/1-2** is not a valid range

Valid values for *type* and *interface*:

- **vlan** *vlan-id*, where *vlan-id* 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 *interface-ranges*.
- **port-channel** *port-channel-number*, where *port-channel-number* is from 1 to 48
- **fastethernet** module/{*first port*} - {*last port*}
- **gigabitethernet** module/{*first port*} - {*last port*}

define interface-range

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 macro1 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 current operating configuration, including defined macros. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

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. |
| /recursive | (Optional) Delete the named directory and all subdirectories and the files contained in it. |
| <i>filesystem:</i> | Alias for a flash file system. The syntax for the local flash file system: flash: |
| <i>/file-url</i> | The path (directory) and filename to delete. |

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

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

If you use the **/force** keyword, you are prompted once at the beginning of the deletion process to confirm the deletion.

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 *Cisco IOS Command Reference for Release 12.1*.

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 filesystem:** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|-------------------------------------|---|
| | archive download-sw | Downloads a new image to the switch and overwrites or keeps the existing image. |

deny (ARP access-list configuration)

Use the **deny** Address Resolution Protocol (ARP) access-list configuration command to deny an ARP packet based on matches against the DHCP bindings. Use the **no** form of this command to remove the specified access control entry (ACE) from the access list.

```
deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

```
no deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|-----------------------------------|---|
| request | (Optional) Define a match for the ARP request. When request is not specified, matching is performed against all ARP packets. |
| ip | Specify the sender IP address. |
| any | Deny any IP or MAC address. |
| host <i>sender-ip</i> | Deny the specified sender IP address. |
| <i>sender-ip sender-ip-mask</i> | Deny the specified range of sender IP addresses. |
| mac | Deny the sender MAC address. |
| host <i>sender-mac</i> | Deny a specific sender MAC address. |
| <i>sender-mac sender-mac-mask</i> | Deny the specified range of sender MAC addresses. |
| response ip | Define the IP address values for the ARP responses. |
| host <i>target-ip</i> | Deny the specified target IP address. |
| <i>target-ip target-ip-mask</i> | Deny the specified range of target IP addresses. |
| mac | Deny the MAC address values for the ARP responses. |
| host <i>target-mac</i> | Deny the specified target MAC address. |
| <i>target-mac target-mac-mask</i> | Deny the specified range of target MAC addresses. |
| log | (Optional) Log a packet when it matches the ACE. |

Defaults

There are no default settings. However, at the end of the ARP access list, there is an implicit **deny ip any mac any** command.

Command Modes

ARP access-list configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

You can add deny clauses to drop ARP packets based on matching criteria.

Examples

This example shows how to define an ARP access list and to deny both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| arp access-list | Defines an ARP access control list (ACL). |
| ip arp inspection filter vlan | Permits ARP requests and responses from a host configured with a static IP address. |
| permit (ARP access-list configuration) | Permits an ARP packet based on matches against the DHCP bindings. |
| show arp access-list | Displays detailed information about ARP access lists. |

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 | larc-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 | larc-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 mask</i> | 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. |
| <i>type mask</i> | (Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. The <i>type</i> 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 <i>cos</i> | (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. |
| larc-sca | (Optional) Select EtherType DEC-LARC-SCA. |

| | |
|-------------------------------------|--|
| lsap <i>lsap-number mask</i> | (Optional) Use the LSAP number (0 to 65535) of a packet with 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 (VINES) 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 2-4](#).

Table 2-4 IPX Filtering Criteria

| IPX Encapsulation Type | | Filter Criterion |
|------------------------|----------------|------------------|
| Cisco IOS Name | Novel Name | |
| 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 |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

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 **host** keyword, you must enter an address mask.

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.

**Note**

For more information about named MAC extended access lists, see the software configuration guide for this release.

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.

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with Ethertype 0x4321:

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

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

Related Commands

| Command | Description |
|---|---|
| mac access-list extended | Creates an access list based on MAC addresses for non-IP traffic. |
| permit (ARP access-list configuration) | Permits non-IP traffic to be forwarded if conditions are matched. |
| show access-lists | Displays access control lists configured on a switch. |

dot1x

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

```
dot1x {system-auth-control} | {guest-vlan supplicant}
```

```
no dot1x {system-auth-control} | {guest-vlan supplicant}
```

Syntax Description

| | |
|------------------------------|---|
| system-auth-control | Enable 802.1x globally on the switch. |
| guest-vlan supplicant | Enable optional guest VLAN behavior globally on the switch. |

Defaults

802.1x is disabled, and the optional guest VLAN behavior is disabled.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|---|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(25)SE | The guest-vlan supplicant keywords were added. |

Usage Guidelines

You must enable authentication, authorization, and accounting (AAA) and specify the authentication method list before globally enabling 802.1x. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Before globally enabling 802.1x on a switch, remove the EtherChannel configuration from the interfaces on which 802.1x and EtherChannel are configured.

If you are using a device running the Cisco Access Control Server (ACS) application for 802.1x authentication with EAP-Transparent LAN Services (TLS) and with EAP-MD5 and your switch is running Cisco IOS Release 12.1(14)EA1, make sure that the device is running ACS Version 3.2.1 or later.

You can use the **guest-vlan supplicant** keywords to enable the optional 802.1x guest VLAN behavior globally on the switch. For more information, see the [dot1x guest-vlan](#) command.

Examples

This example shows how to globally enable 802.1x on a switch:

```
Switch(config)# dot1x system-auth-control
```

This example shows how to globally enable the optional guest VLAN behavior on a switch:

```
Switch(config)# dot1x guest-vlan supplicant
```

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

| Related Commands | Command | Description |
|------------------|--|--|
| | dot1x guest-vlan | Enables and specifies an active VLAN as an 802.1x guest VLAN. |
| | dot1x port-control | Enables manual control of the authorization state of the port. |
| | show dot1x [interface <i>interface-id</i>] | Displays 802.1x status for the specified port. |

dot1x default

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

dot1x default

Syntax Description

This command has no arguments or keywords.

Defaults

These are the default values:

- The per-port 802.1x protocol enable state is disabled (force-authorized).
- The number of seconds between re-authentication attempts is 3600 seconds.
- The periodic re-authentication is disabled.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The host mode is single host.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Examples

This example shows how to reset the configurable 802.1x parameters on a port:

```
Switch(config-if)# dot1x default
```

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

Related Commands

| Command | Description |
|--|--|
| show dot1x [interface interface-id] | Displays 802.1x status for the specified port. |

dot1x guest-vlan

Use the **dot1x guest-vlan** interface configuration command to specify an active VLAN as an 802.1x guest VLAN. Use the **no** form of this command to return to the default setting.

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

Syntax Description

vlan-id Specify an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.

Defaults

No guest VLAN is configured.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|--|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(25)SE | This command was modified to change the default guest VLAN behavior. |

Usage Guidelines

For each 802.1x port on the switch, you can configure a guest VLAN to provide limited services to clients (a device or workstation connected to the switch), such as downloading the 802.1x client software. These users might be upgrading their systems for 802.1x authentication, and some hosts, such as Windows 98 systems, might not be 802.1x-capable.

When you enable a guest VLAN on an 802.1x port, the switch assigns clients to a guest VLAN when the authentication server does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.

Before Cisco IOS Release 12.2(25)SE, the switch did not maintain the EAPOL packet history and allowed clients that failed authentication access to the guest VLAN, regardless of whether EAPOL packets had been detected on the interface. You can use the **dot1x guest-vlan supplicant** global configuration command to enable this optional behavior.

With Cisco IOS Release 12.2(25)SE and later, the switch maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, network access is denied. The EAPOL history is reset upon loss of link.

Any number of non-802.1x-capable clients are allowed access when the switch port is moved to the guest VLAN. If an 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on 802.1x ports in single-host or multiple-hosts mode.

You can configure any active VLAN except an RSPAN VLAN, private VLAN, or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

After you configure a guest VLAN for an 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can also change the settings for restarting the 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the 802.1x authentication process (802.1x quiet period and switch-to-client transmission time).

Examples

This example shows how to specify VLAN 5 as an 802.1x guest VLAN:

```
Switch(config-if)# dot1x guest-vlan 5
```

This example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request, and to enable VLAN 2 as an 802.1x guest VLAN when an 802.1X port is connected to a DHCP client:

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

This example shows how to enable the optional guest VLAN behavior and to specify VLAN 5 as an 802.1x guest VLAN:

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x guest-vlan 5
```

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

Related Commands

| Command | Description |
|---|---|
| dot1x | Enables the optional guest VLAN supplicant feature. |
| show dot1x [interface interface-id] | Displays 802.1x status for the specified port. |

dot1x host-mode

Use the **dot1x host-mode** interface configuration command to allow a single host (client) or multiple hosts on an 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-host mode on the switch. |

Defaults

The default is single-host mode.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Use this command to limit an 802.1x-enabled port to a single client or to attach multiple clients to an 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.

Before entering this command, make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified port.

Examples

This example shows how to enable 802.1x globally, to enable 802.1x on a port, and to enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

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

Related Commands

| Command | Description |
|---|--|
| <code>show dot1x [interface <i>interface-id</i>]</code> | Displays 802.1x status for the specified port. |

dot1x initialize

Use the **dot1x initialize** privileged EXEC command to manually return the specified 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 <i>interface-id</i> Port to be initialized. |
|---------------------------|--|

| | |
|-----------------|------------------------------|
| Defaults | There is no default setting. |
|-----------------|------------------------------|

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

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | <p>Use this command to initialize the 802.1x state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.</p> <p>There is no no form of this command.</p> |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | <p>This example shows how to manually initialize a port:</p> <pre>Switch# dot1x initialize interface gigabitethernet0/2</pre> |
|-----------------|---|

You can verify the unauthorized port status by entering the **show dot1x [interface interface-id]** privileged EXEC command.

| Related Commands | Command | Description |
|-------------------------|--|--|
| | show dot1x [interface interface-id] | Displays 802.1x status for the specified port. |

dot1x max-reauth-req

Use the **dot1x max-reauth-req** interface configuration command on the switch stack or on a standalone switch 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

| | |
|--------------|--|
| <i>count</i> | Number of times that the switch restarts the authentication process before the port 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(18)SE | 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.

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

Related Commands

| Command | Description |
|---|--|
| dot1x max-req | Sets the maximum number of times that the switch forwards an EAP-request/identity 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. |
| show dot1x [interface interface-id] | Displays 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)-request/identity frame (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 | <i>count</i> | Number of times that the switch sends an EAP-request/identity frame 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 |
| | 12.1(19)EA1 | 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. |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | This example shows how to set 5 as the number of times that the switch sends an EAP-request/identity frame before restarting the authentication process: |
|-----------------|--|

```
Switch(config-if)# dot1x max-req 5
```

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

| | | |
|-------------------------|---|--|
| Related Commands | Command | Description |
| | dot1x timeout <i>tx-period</i> | 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. |
| | show dot1x [interface <i>interface-id</i>] | Displays 802.1x status for the specified port. |

dot1x multiple-hosts

This is an obsolete command.

In past releases, the **dot1x multiple-hosts** interface configuration command was used to allow multiple hosts (clients) on an 802.1x-authorized port.

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Related Commands

| Command | Description |
|---------------------------------|---|
| dot1x host-mode | Sets the 802.1x host mode on a port. |
| show dot1x | Displays 802.1x statistics, administrative status, and operational status for the switch or for the specified port. |

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 | force-authorized | force-unauthorized}

no dot1x port-control

Syntax Description

| | |
|---------------------------|--|
| auto | Enable 802.1x authentication on the port and cause the port to change to the authorized or unauthorized state based on the 802.1x authentication exchange between the switch and the client. |
| force-authorized | Disable 802.1x authentication on the port and cause the port to transition to the authorized state without an authentication exchange. The port sends and receives normal traffic without 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-authorized.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

You must globally enable 802.1x on the switch by using the **dot1x system-auth-control** global configuration command before enabling 802.1x on a specific port.

The 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN ports, and Layer 3 routed ports.

You can use the **auto** keyword only if the port is not configured as one of these:

- Trunk port—If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, an error message appears, and the port mode is not changed.
- Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x on a dynamic port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.
- Dynamic-access ports—If you try to enable 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

- EtherChannel port—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x on an EtherChannel port, an error message appears, and 802.1x is not enabled.



Note In software releases earlier than Cisco IOS Release 12.2(18)SE, if 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1x on a port that is a SPAN or RSPAN destination port. However, 802.1x is disabled until the port is removed as a SPAN or RSPAN destination. You can enable 802.1x on a SPAN or RSPAN source port.

To globally disable 802.1x on the switch, use the **no dot1x system-auth-control** global configuration command. To disable 802.1x on a specific port, use the **no dot1x port-control** interface configuration command.

Examples

This example shows how to enable 802.1x on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
```

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

Related Commands

| Command | Description |
|--|--|
| show dot1x [interface interface-id] | Displays 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 all 802.1x-enabled ports or the specified 802.1x-enabled port.

dot1x re-authenticate interface *interface-id*

| | |
|---------------------------|--|
| Syntax Description | interface <i>interface-id</i> Module and port number of the interface to re-authenticate. |
|---------------------------|--|

| | |
|-----------------|------------------------------|
| Defaults | There is no default setting. |
|-----------------|------------------------------|

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

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.1(19)EA1 | 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# dot1x re-authenticate interface gigabitethernet0/1
```

dot1x re-authentication

This is an obsolete command.

In past releases, the **dot1x re-authentication** global configuration command was used to set the amount of time between periodic re-authentication attempts.

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Related Commands

| Command | Description |
|--|---|
| dot1x reauthentication | Sets the number of seconds between re-authentication attempts. |
| show dot1x | Displays 802.1x statistics, administrative status, and operational status for the switch or for the specified port. |

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 |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | 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)# dot1x reauthentication
Switch(config-if)# dot1x 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. |
| | show dot1x [interface <i>interface-id</i>] | Displays 802.1x status for the specified port. |

dot1x timeout

Use the **dot1x timeout** interface configuration command to set 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 <i>seconds</i> | 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 <i>seconds</i> | Number of seconds between re-authentication attempts. The range is 1 to 65535. |
| server-timeout <i>seconds</i> | 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 <i>seconds</i> | Number of seconds that the switch waits for the retransmission of packets by the switch to the 802.1x client. The range is 30 to 65535. |
| tx-period <i>seconds</i> | 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 settings:

reauth-period is 3600 seconds.

quiet-period is 60 seconds.

tx-period is 30 seconds.

supp-timeout is 30 seconds.

server-timeout is 30 seconds.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|--|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(20)SE | The ranges for the server-timeout , supp-timeout , and tx-period keywords were changed. |

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.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a smaller number 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 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 **auto** for Fast Ethernet and Gigabit Ethernet ports and for 1000BASE-T small form-factor pluggable (SFP) modules.

The default is **half** for 100BASE-FX MMF SFP modules.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

This command is not available on SFP module ports unless a 1000BASE-T SFP module or a 100BASE-FX MMF SFP module is in the port. All other SFP modules operate only in full-duplex mode.

- When a 1000BASE-T SFP module is in the SFP module port, you can configure duplex mode to **auto** or **full**.
- When a 100BASE-FX SFP module is in the SFP module port, 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 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.

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.



Note 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.

Beginning with Cisco IOS Release 12.2(20)SE1, you can configure the duplex setting when the speed is set to **auto**.

**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 configuration guide 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
```

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

Related Commands

| Command | Description |
|---------------------------------|---|
| show interfaces | Displays the interface settings on the switch. |
| speed | Sets the speed on a 10/100 or 10/100/1000 Mbps interface. |

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 | arp-inspection | dhcp-rate-limit | dtp-flap | gbic-invalid |
l2ptguard | link-flap | loopback | pagp-flap}
```

```
no errdisable detect cause {all | arp-inspection | dhcp-rate-limit | dtp-flap | gbic-invalid |
l2ptguard | link-flap | pagp-flap}
```

| Syntax Description | | |
|------------------------|---|--|
| all | Enable error detection for all error-disable causes. | |
| arp-inspection | Enable error detection for dynamic Address Resolution Protocol (ARP) inspection. | |
| dhcp-rate-limit | Enable error detection for DHCP snooping. | |
| dtp-flap | Enable error detection for the Dynamic Trunking Protocol (DTP) flapping. | |
| gbic-invalid | Enable error detection for an invalid Gigabit Interface Converter (GBIC) module. Note On the Catalyst 33560 switch, this error refers to an invalid small form-factor pluggable (SFP) module. | |
| l2ptguard | Enable error detection for a Layer 2 protocol-tunnel error-disabled cause. | |
| 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. | |

Defaults Detection is enabled for all causes.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------|--|
| | 12.1(19)EA1 | This command was introduced. |
| | 12.2(20)SE | The arp-inspection keyword was added. |
| | 12.2(25)SE | The l2ptguard keyword was added. |

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 **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

Examples

This example shows 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. |

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 | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap |
psecure-violation | security-violation | udld | vmps} | {interval interval}}
```

```
no errdisable recovery {cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | loopback | pagp-flap |
psecure-violation | security-violation | udld | 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. |
| arp-inspection | Enable the timer to recover from the Address Resolution Protocol (ARP) inspection 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. |
| dtp-flap | Enable the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disable state. |
| gbic-invalid | Enable the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disable state. Note On the Catalyst 3560 switch, this error refers to an invalid small form-factor pluggable (SFP) error-disable state. |
| l2ptguard | Enable the timer to recover from a Layer 2 protocol tunnel error-disabled 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 802.1x-violation disabled state |
| udld | Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state. |

| | |
|---------------------------------|--|
| vmpls | Enable the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state. |
| interval <i>interval</i> | 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. |

**Note**

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

Defaults

Recovery is disabled for all causes.
The default recovery interval is 300 seconds.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|---|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(18)SE | The channel-misconfig keyword was added. |
| 12.2(20)SE | The arp-inspection keyword was added. |
| 12.2(25)SE | The l2ptguard keyword was added. |

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 must enter the **shutdown** then **no shutdown** commands to manually recover an interface from the error-disabled state.

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.

■ errdisable recovery

| Related Commands | Command | Description |
|------------------|---|--|
| | show errdisable recovery | Displays errdisable recovery timer information. |
| | show interfaces status err-disabled | Displays interface status or a list of interfaces in error-disabled state. |

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 }



Note

The Catalyst 3560 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 |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The switch does not support sending flow-control pause frames.

Note that the **on** and **desired** keywords have the same result.

When you use the **flowcontrol** command to set a port to control traffic rates during congestion, you are setting flow control on a port to one of these conditions:

- **receive on** or **desired**: The port cannot send out pause frames, but can operate with an attached device that is required to or is able to send pause frames; the port is able to receive pause frames.
- **receive off**: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner and no pause frames are sent or received by either device.

Table 2-5 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 2-5 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*

Syntax Description

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 |
|-------------|---|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(25)SE | The <i>port-channel-number</i> range was changed from 1 to 12 to 1 to 48. |

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. You should manually configure the port-channel logical interface before putting the interface into the channel group.

Only one port channel in a channel group is allowed.



Caution

When using a port-channel interface as a routed port, do not assign Layer 3 addresses on the physical ports that are assigned to the channel group.



Caution

Do not assign bridge groups on the physical ports in a channel group used as a Layer 3 port-channel interface because it creates loops. You must also disable spanning tree.

interface port-channel

Follow these guidelines when you use the **interface port-channel** command:

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the physical port and not on the port-channel interface.
- Do not configure a port that is an active member of an EtherChannel as an 802.1x port. If 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 configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Examples

This example shows how to create a port-channel interface with a port channel number of 5:

```
Switch(config)# interface port-channel 5
```

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 current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

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

| | |
|-------------------|--|
| <i>port-range</i> | 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 has no default setting.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

When you enter interface range configuration mode, all interface parameters you enter are attributed to all interfaces within the range.

For VLANs, you can use the **interface range** command only on existing VLAN switch virtual interfaces (SVIs). To display VLAN SVIs, enter the **show running-config** privileged EXEC command. VLANs not displayed cannot be used in the **interface range** command. The commands entered under **interface range** command 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 the interface range in two ways:

- Specifying up to five interface ranges
- Specifying 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 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:

- 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 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 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 *macro1* for the same function. The advantage is that you can reuse *macro1* until you delete it.

```
Switch(config)# define interface-range macro1 gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```


Related Commands

| Command | Description |
|--|--|
| define interface-range | Creates an interface range macro. |
| show running-config | Displays the configuration information currently running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

interface vlan

Use the **interface vlan** global configuration command to create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode. Use the **no** form of this command to delete an SVI.

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 |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

SVIs are created the first time that you enter the **interface vlan** *vlan-id* command for a particular *vlan*. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an ISL or 802.1Q encapsulated trunk or the VLAN ID configured for an access port.



Note

When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI by entering the **no interface vlan** *vlan-id* 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.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but much of the previous configuration will be gone.

The interrelationship between the number of SVIs configured on a switch and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables. For more information, see the [sdm prefer](#) command.

Examples

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

You can verify your setting by entering the **show interfaces** and **show interfaces vlan *vlan-id*** privileged EXEC commands.

| Related Commands | Command | Description |
|------------------|---|---|
| | show interfaces vlan <i>vlan-id</i> | Displays the administrative and operational status of all interfaces or the specified VLAN. |

ip access-group

Use the **ip access-group** interface configuration command to control access to a Layer 2 or Layer 3 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 | out}
```

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

Syntax Description

| | |
|---------------------------|---|
| <i>access-list-number</i> | The number of the IP access control list (ACL). The range is 1 to 199 or 1300 to 2699. |
| <i>name</i> | The name of an IP ACL, specified in the ip access-list global configuration command. |
| in | Specify filtering on inbound packets. |
| out | Specify filtering on outbound packets. This keyword is valid only on Layer 3 interfaces. |

Defaults

No access list is applied to the interface.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

You can apply named or numbered standard or extended IP access lists to an interface. To define an access list by name, use the **ip access-list** global configuration command. To define a numbered access list, use the **access list** global configuration command. You can use numbered standard access lists ranging from 1 to 99 and 1300 to 1999 or extended access lists ranging from 100 to 199 and 2000 to 2699.

You can use this command to apply an access list to a Layer 2 or Layer 3 interface. However, note these limitations for Layer 2 interfaces (port ACLs):

- You can only apply ACLs in the inbound direction; the **out** keyword is not supported for Layer 2 interfaces.
- You can only apply one IP ACL and one MAC ACL per interface.
- Layer 2 interfaces do not support logging; if the **log** keyword is specified in the IP ACL, it is ignored.
- An IP ACL applied to a Layer 2 interface only filters IP packets. To filter non-IP packets, use the **mac access-group** interface configuration command with MAC extended ACLs.

You can use router ACLs, input port ACLs, and VLAN maps on the same switch. However, a port ACL takes precedence over a router ACL or VLAN map.

- When an input port ACL is applied to an interface and a VLAN map is applied to a VLAN that the interface is a member of, incoming packets received on ports with the ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.
- When an input router ACL and input port ACLs exist in an switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.
- When a VLAN map, input router ACLs, and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.
- When a VLAN map, output router ACLs, and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Outgoing routed IP packets are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

You can apply IP ACLs to both outbound or inbound Layer 3 interfaces.

A Layer 3 interface can have one IP ACL applied in each direction.

You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.

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 access list has been applied to a Layer 3 interface, discarding a packet (by default) causes the generation of an Internet Control Message Protocol (ICMP) Host Unreachable message. ICMP Host Unreachable messages are not generated for packets discarded on a Layer 2 interface.

For standard outbound access lists, after receiving a packet and sending it to a controlled interface, the switch checks the packet against the access list. If the access list permits the packet, the switch sends the packet. If the access list denies the packet, the switch discards the packet and, by default, generates an ICMP Host Unreachable message.

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 access-lists | Displays IP ACLs configured on the switch. For syntax information, select Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands. |
| | 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 or an IP address for each switch virtual interface (SVI) or routed port on the Layer 3 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

| | |
|--------------------|---|
| <i>ip-address</i> | IP address. |
| <i>subnet-mask</i> | 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 defined.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

If you remove the switch IP address through a Telnet session, your connection to the switch will be lost.

Hosts can find subnet masks using the Internet Control Message Protocol (ICMP) Mask Request 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.

You can use the optional keyword **secondary** to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.



Note

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.

When you are routing Open Shortest Path First (OSPF), ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

If your switch receives its IP address from a Bootstrap Protocol (BOOTP) or a DHCP server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or the DHCP server cannot reassign the address.

A Layer 3 switch can have an IP address assigned to each routed port and SVI. The number of routed ports and SVIs that you can configure is not limited by software; however, the interrelationship between this number and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables. For more information, see the **sdm prefer** command.

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 172.20.128.2 255.255.255.0
```

This example shows how to configure the IP address for a port on the Layer 3 switch:

```
Switch(config)# ip multicast-routing
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

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

Related Commands

| Command | Description |
|----------------------------|--|
| show running-config | Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

ip arp inspection filter vlan

Use the **ip arp inspection filter vlan** global configuration command to permit or deny Address Resolution Protocol (ARP) requests and responses from a host configured with a static IP address when dynamic ARP inspection is enabled. Use the **no** form of this command to return to the default settings.

ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

no ip arp inspection filter *arp-acl-name* **vlan** *vlan-range* [**static**]

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|---------------------|---|
| <i>arp-acl-name</i> | ARP access control list (ACL) name. |
| <i>vlan-range</i> | VLAN number or range. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| static | (Optional) Specify static to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used. If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL. |

Defaults

No defined ARP ACLs are applied to any VLAN.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

When an ARP ACL is applied to a VLAN for dynamic ARP inspection, only the ARP packets with IP-to-MAC address bindings are compared against the ACL. If the ACL permits a packet, the switch forwards it. All other packet types are bridged in the ingress VLAN without validation.

If the switch denies a packet because of an explicit deny statement in the ACL, the packet is dropped. If the switch denies a packet because of an implicit deny statement, the packet is then compared against the list of DHCP bindings (unless the ACL is *static*, which means that packets are not compared against the bindings).

Use the **arp access-list** *acl-name* global configuration command to define the ARP ACL or to add clauses to the end of a predefined list.

Examples

This example shows how to apply the ARP ACL *static-hosts* to VLAN 1 for dynamic ARP inspection:

```
Switch(config)# ip arp inspection filter static-hosts vlan 1
```

You can verify your settings by entering the **show ip arp inspection vlan 1** privileged EXEC command.

Related Commands

| Command | Description |
|---|--|
| arp access-list | Defines an ARP ACL. |
| deny (ARP access-list configuration) | Denies an ARP packet based on matches against the DHCP bindings. |
| permit (ARP access-list configuration) | Permits an ARP packet based on matches against the DHCP bindings. |
| show arp access-list | Displays detailed information about ARP access lists. |
| show ip arp inspection vlan <i>vlan-range</i> | Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. |

ip arp inspection limit

Use the **ip arp inspection limit** interface configuration command to limit the rate of incoming Address Resolution Protocol (ARP) requests and responses on an interface. It prevents dynamic ARP inspection from using all of the switch resources if a denial-of-service attack occurs. Use the **no** form of this command to return to the default settings.

ip arp inspection limit {rate *pps* [**burst interval** *seconds*] | **none**}

no ip arp inspection limit

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|--------------------------------------|---|
| rate <i>pps</i> | Specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 packets per second (pps). |
| burst interval <i>seconds</i> | (Optional) Specify the consecutive interval in seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15 seconds. |
| none | Specify no upper limit for the rate of incoming ARP packets that can be processed. |

Defaults

The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second.

The rate is unlimited on all trusted interfaces.

The burst interval is 1 second.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

The rate applies to both trusted and untrusted interfaces. Configure appropriate rates on trunks to process packets across multiple dynamic ARP inspection-enabled VLANs, or use the **none** keyword to make the rate unlimited.

After a switch receives more than the configured rate of packets every second consecutively over a number of burst seconds, the interface is placed into an error-disabled state.

Unless you explicitly configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the **no ip arp inspection limit** interface configuration command, the interface reverts to its default rate limit.

You should configure trunk ports with higher rates to reflect their aggregation. When the rate of incoming packets exceeds the user-configured rate, the switch places the interface into an error-disabled state. The error-disable recovery feature automatically removes the port from the error-disabled state according to the recovery setting.

The rate of incoming ARP packets on EtherChannel ports equals the sum of the incoming rate of ARP packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on all the channel members.

Examples

This example shows how to limit the rate of incoming ARP requests on a port to 25 pps and to set the interface monitoring interval to 5 consecutive seconds:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection limit rate 25 burst interval 5
```

You can verify your settings by entering the **show ip arp inspection interfaces** *interface-id* privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| show ip arp inspection interfaces | Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces. |

ip arp inspection log-buffer

Use the **ip arp inspection log-buffer** global configuration command to configure the dynamic Address Resolution Protocol (ARP) inspection logging buffer. Use the **no** form of this command to return to the default settings.

```
ip arp inspection log-buffer { entries number | logs number interval seconds }
```

```
no ip arp inspection log-buffer { entries | logs }
```

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|--------------------------------|--|
| entries <i>number</i> | Number of entries to be logged in the buffer. The range is 0 to 1024. |
| logs <i>number</i> | Number of entries needed in the specified interval to generate system messages. |
| interval <i>seconds</i> | For logs <i>number</i> , the range is 0 to 1024. A 0 value means that the entry is placed in the log buffer, but a system message is not generated. For interval <i>seconds</i> , the range is 0 to 86400 seconds (1 day). A 0 value means that a system message is immediately generated (and the log buffer is always empty). |

Defaults

When dynamic ARP inspection is enabled, denied or dropped ARP packets are logged.

The number of log entries is 32.

The number of system messages is limited to 5 per second.

The logging-rate interval is 1 second.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

A value of 0 is not allowed for both the **logs** and the **interval** keywords.

The **logs** and **interval** settings interact. If the **logs** *number* X is greater than **interval** *seconds* Y, X divided by Y (X/Y) system messages are sent every second. Otherwise, one system message is sent every Y divided by X (Y/X) seconds. For example, if the **logs** *number* is 20 and the **interval** *seconds* is 4, the switch generates system messages for five entries every second while there are entries in the log buffer.

A log buffer entry can represent more than one packet. For example, if an interface receives many packets on the same VLAN with the same ARP parameters, the switch combines the packets as one entry in the log buffer and generates a system message as a single entry.

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

Examples

This example shows how to configure the logging buffer to hold up to 45 entries:

```
Switch(config)# ip arp inspection log-buffer entries 45
```

This example shows how to configure the logging rate to 20 log entries per 4 seconds. With this configuration, the switch generates system messages for five entries every second while there are entries in the log buffer.

```
Switch(config)# ip arp inspection log-buffer logs 20 interval 4
```

You can verify your settings by entering the **show ip arp inspection log** privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| arp access-list | Defines an ARP access control list (ACL). |
| clear ip arp inspection log | Clears the dynamic ARP inspection log buffer. |
| ip arp inspection vlan logging | Controls the type of packets that are logged per VLAN. |
| show ip arp inspection log | Displays the configuration and contents of the dynamic ARP inspection log buffer. |

ip arp inspection trust

Use the **ip arp inspection trust** interface configuration command to configure an interface trust state that determines which incoming Address Resolution Protocol (ARP) packets are inspected. Use the **no** form of this command to return to the default setting.

ip arp inspection trust

no ip arp inspection trust

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description This command has no arguments or keywords.

Defaults The interface is untrusted.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|------------|------------------------------|
| | 12.2(20)SE | This command was introduced. |

Usage Guidelines The switch does not check ARP packets that it receives on the trusted interface; it simply forwards the packets.

For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection vlan logging** global configuration command.

Examples This example shows how to configure a port to be trusted:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```

You can verify your setting by entering the **show ip arp inspection interfaces *interface-id*** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|---|---|
| | ip arp inspection log-buffer | Configures the dynamic ARP inspection logging buffer. |
| | show ip arp inspection interfaces | Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces. |
| | show ip arp inspection log | Displays the configuration and contents of the dynamic ARP inspection log buffer. |

ip arp inspection validate

Use the **ip arp inspection validate** global configuration command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to return to the default settings.

ip arp inspection validate {[src-mac] [dst-mac] [ip]}

no ip arp inspection validate [src-mac] [dst-mac] [ip]

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|----------------|---|
| src-mac | Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped. |
| dst-mac | Compare the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped. |
| ip | Compare the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are compared in all ARP requests and responses. Target IP addresses are checked only in ARP responses. |

Defaults

No checks are performed.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables **src-mac** and **dst-mac** validations, and a second command enables IP validation only, the **src-mac** and **dst-mac** validations are disabled as a result of the second command.

If you first specify the **src-mac** keyword, you also can specify the **dst-mac** and **ip** keywords. If you first specify the **ip** keyword, no other keywords can be specified.

The **no** form of the command disables only the specified checks. If none of the options are enabled, all checks are disabled.

Examples

This example show how to enable source MAC validation:

```
Switch(config)# ip arp inspection validate src-mac
```

You can verify your setting by entering the **show ip arp inspection vlan** *vlan-range* privileged EXEC command.

Related Commands

| Command | Description |
|--|--|
| show ip arp inspection vlan <i>vlan-range</i> | Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. |

ip arp inspection vlan

Use the **ip arp inspection vlan** global configuration command to enable dynamic Address Resolution Protocol (ARP) inspection on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|-------------------|---|
| <i>vlan-range</i> | VLAN number or range. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
|-------------------|---|

Defaults

ARP inspection is disabled on all VLANs.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

You must specify the VLANs on which to enable dynamic ARP inspection.

Dynamic ARP inspection is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.

Examples

This example shows how to enable dynamic ARP inspection on VLAN 1:

```
Switch(config)# ip arp inspection vlan 1
```

You can verify your setting by entering the **show ip arp inspection vlan** *vlan-range* privileged EXEC command.

| Related Commands | Command | Description |
|------------------|---|--|
| | arp access-list | Defines an ARP access control list (ACL). |
| | show ip arp inspection vlan <i>vlan-range</i> | Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. |

ip arp inspection vlan logging

Use the **ip arp inspection vlan logging** global configuration command to control the type of packets that are logged per VLAN. Use the **no** form of this command to disable this logging control.

```
ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit}}
```

```
no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings}
```

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|---|--|
| <i>vlan-range</i> | Specify the VLANs configured for logging. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| acl-match { matchlog none } | Specify that the logging of packets is based on access control list (ACL) matches. The keywords have these meanings: <ul style="list-style-type: none"> matchlog—Log packets based on the logging configuration specified in the access control entries (ACE). If you specify the matchlog keyword in this command and the log keyword in the permit or deny ARP access-list configuration command, Address Resolution Protocol (ARP) packets permitted or denied by the ACL are logged. none—Do not log packets that match ACLs. |
| dhcp-bindings { permit all none } | Specify the logging of packets is based on Dynamic Host Configuration Protocol (DHCP) binding matches. The keywords have these meanings: <ul style="list-style-type: none"> all—Log all packets that match DHCP bindings. none—Do not log packets that match DHCP bindings. permit—Log DHCP-binding permitted packets. |

Defaults

All denied or all dropped packets are logged.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

The term *logged* means that the entry is placed into the log buffer and that a system message is generated. The **acl-match** and **dhcp-bindings** keywords merge with each other; that is, when you configure an ACL match, the DHCP bindings configuration is not disabled. Use the **no** form of the command to reset the logging criteria to their defaults. If neither option is specified, all types of logging are reset to log when ARP packets are denied. These are the options:

- **acl-match**—Logging on ACL matches is reset to log on deny.
- **dhcp-bindings**—Logging on DHCP binding matches is reset to log on deny.

If neither the **acl-match** or the **dhcp-bindings** keywords are specified, all denied packets are logged.

The implicit deny at the end of an ACL does not include the **log** keyword. This means that when you use the **static** keyword in the **ip arp inspection filter vlan** global configuration command, the ACL overrides the DHCP bindings. Some denied packets might not be logged unless you explicitly specify the **deny ip any mac any log** ACE at the end of the ARP ACL.

Examples

This example shows how to configure ARP inspection on VLAN 1 to log packets that match the **permit** commands in the ACL:

```
Switch(config)# arp access-list test1
Switch(config-arp-nacl)# permit request ip any mac any log
Switch(config-arp-nacl)# permit response ip any any mac any any log
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

You can verify your settings by entering the **show ip arp inspection vlan** *vlan-range* privileged EXEC command.

Related Commands

| Command | Description |
|---|--|
| arp access-list | Defines an ARP ACL. |
| clear ip arp inspection log | Clears the dynamic ARP inspection log buffer. |
| ip arp inspection log-buffer | Configures the dynamic ARP inspection logging buffer. |
| show ip arp inspection log | Displays the configuration and contents of the dynamic ARP inspection log buffer. |
| show ip arp inspection vlan <i>vlan-range</i> | Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. |

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 |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines For 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*

This command is available only if your switch is running the enhanced multilayer image (EMI).

| Syntax Description | | |
|--------------------------------------|--|--|
| <i>mac-address</i> | Specify a MAC address. | |
| vlan <i>vlan-id</i> | Specify a VLAN number. The range is from 1 to 4904. | |
| <i>ip-address</i> | Specify an IP address. | |
| interface <i>interface-id</i> | Specify an interface on which to add or delete a binding entry. | |
| expiry <i>seconds</i> | 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 defined.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|------------------------------|
| | 12.2(20)SE | This command was introduced. |

Usage Guidelines 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.

When a switch learns new bindings or it loses bindings, the switch updates the entries in the database and in the binding file at a configured location. The frequency at which the database and the file are updated is based on a configurable delay, and the updates are batched. You can configure this delay by using the **ip dhcp snooping database write-delay** *seconds* global configuration command.

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 binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet0/1 expiry 1000
```

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

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. |
| show ip source binding | Displays the dynamically and statically configured bindings in the DHCP snooping binding database. |

ip dhcp snooping database

Use the **ip dhcp snooping database** global configuration command to configure the DHCP snooping binding database agent or the binding file. Use the **no** form of this command to delete the agent or file specified by the URL, 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]
```

This command is available only if your switch is running the enhanced multilayer image (EMI).

| Syntax Description | | |
|--|--|--|
| flash: / <i>filename</i> | | Specify that the database agent or the binding file is in the flash memory. |
| ftp: // <i>user:password@host/filename</i> | | Specify that the database agent or the binding file is on an FTP server. |
| http: //[[<i>username:password</i>]@][<i>hostname</i> <i>host-ip</i>][/ <i>directory</i>]/ <i>image-name.tar</i> | | Specify that the database agent or the binding file is on an FTP server. |
| rcp: // <i>user@host/filename</i> | | Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server. |
| tftp: // <i>host/filename</i> | | Specify that the database agent or the binding file is on a TFTP server. |
| timeout <i>seconds</i> | | 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 <i>seconds</i> | | 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. |

Defaults

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 History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

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 not configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

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 **ip dhcp snooping database flash:/filename** command to save the DHCP snooping binding database in the stack master NVRAM. The database is not saved in a stack member NVRAM.

Use the **no ip dhcp snooping database** command to delete the agent or file specified by the URL.

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 *directory*. A file named *file* must be present on the TFTP server.

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

This example shows how to store a binding file called file01.txt in the stack master NVRAM.

```
Switch(config)# ip dhcp snooping database flash:file01.txt
```

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

Related Commands

| Command | Description |
|--|--|
| ip dhcp 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. |

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 |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | 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 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 | <i>rate</i> | Number of DHCP messages an interface can receive per second. The range is 1 to 2048. |
|---------------------------|-------------|--|

Defaults DHCP snooping rate limiting is disabled.

Command Modes Interface configuration

| Command History | Release | Modification |
|------------------------|----------------|-------------------------------------|
| | 12.1(19)EA1 | This command was introduced. |
| | 12.2(18)SE | The range was changed to 1 to 2048. |

Usage Guidelines Normally, the rate limit applies to untrusted interfaces. If you want to configure rate limiting for trusted interfaces, keep in mind that trusted interfaces might aggregate DHCP traffic on multiple VLANs (some of which might not be snooped) in the switch, and you will need to adjust the interface rate limits to a higher value.

If the rate limit is exceeded, the interface is error-disabled. If you enabled error recovery by entering the **errdisable recovery dhcp-rate-limit** global configuration command, the interface retries the operation again when all the causes have timed out. If the error-recovery mechanism is not enabled, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

Examples This example shows how to set a message rate limit of 150 messages per second on an interface:

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

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

| Related Commands | Command | Description |
|-------------------------|---|---|
| | errdisable recovery | Configures the recover mechanism. |
| | show ip dhcp snooping | Displays the DHCP snooping configuration. |
| | show ip dhcp snooping binding | Displays the DHCP snooping binding information. |

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 trust is disabled.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines Configure as trusted ports those that are connected to a DHCP server or to other switches or routers. Configure as untrusted ports those that are connected to DHCP clients.

Examples This example shows how to enable DHCP snooping trust on a port:

```
Switch(config-if)# ip dhcp snooping trust
```

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 verify

Use the **ip dhcp snooping verify** 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

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | 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 <i>vlan-range</i> | Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping. The range is 1 to 4094. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space. |
|-------------------------------|---|

Defaults

DHCP snooping is disabled on all VLANs.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

You must first globally enable DHCP snooping before enabling DHCP snooping on a VLAN.

Examples

This example shows how to enable DHCP snooping on VLAN 10:

```
Switch(config)# ip dhcp snooping vlan 10
```

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 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 | <i>profile number</i> The IGMP profile number to be applied. The range is 1 to 4294967295. |
|---------------------------|--|

| | |
|-----------------|------------------------------|
| Defaults | No IGMP filters are applied. |
|-----------------|------------------------------|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | <p>You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.</p> <p>An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.</p> |
|-------------------------|---|

| | |
|-----------------|--|
| Examples | This example shows how to apply IGMP profile 22 to a port. |
|-----------------|--|

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 22
```

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

| Related Commands | Command | Description |
|-------------------------|--|---|
| | ip igmp profile | Configures the specified IGMP profile number. |
| | show ip igmp profile | Displays the characteristics of the specified IGMP profile. |
| | show running-config interface interface-id | 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

| | |
|-----------------------|--|
| <i>number</i> | 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, remove an randomly-selected entry in the forwarding table and add an entry for the next IGMP group. |

Defaults

The default maximum number of groups is no limit.

After the switch learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or 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.

- If you configure the throttling action as **replace** and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch deletes a randomly-selected entry and adds an entry for the next IGMP report received on the interface.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups {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 delete a random IGMP group in the forwarding table and to add an entry for the IGMP group 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 |
|---|--|
| show running-config interface interface-id | Displays the running configuration on the switch interface, including 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*

Syntax Description

profile number The IGMP profile number being configured. The range is 1 to 4294967295.

Defaults

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | 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 range with a start and an end address.

When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one 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 your settings by using the **show ip igmp profile** privileged EXEC command.

■ ip igmp profile

| Related Commands | Command | Description |
|------------------|--------------------------------------|---|
| | ip igmp filter | Applies the IGMP profile to the specified interface. |
| | show ip igmp profile | 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 VLAN. Use the command with keywords to enable and configure IGMP snooping on a VLAN interface. Use the **no** form of this command to disable IGMP snooping or to reset the parameters to the default settings.

```
ip igmp snooping [vlan vlan-id [immediate-leave | mrouter {interface interface-id | learn {cgmp | pim-dvmrp}}] | static ip-address interface interface-id]]
```

```
no ip igmp snooping [vlan vlan-id [immediate-leave | mrouter {interface interface-id | learn {cgmp | pim-dvmrp}}] | static ip-address interface interface-id]]
```

Syntax Description

| | |
|--------------------------------------|---|
| vlan <i>vlan-id</i> | (Optional) When used with other keywords, enable IGMP snooping on a VLAN interface. Use the no form of this command to disable IGMP snooping on a VLAN interface. The range is 1 to 4094. |
| immediate-leave | (Optional) Enable IGMP immediate-leave processing on a VLAN interface. Use the no form of the command to disable the Immediate Leave feature on the interface. |
| mrouter | (Optional) Add a multicast router port or configure the multicast router learning method. The no form of the command removes the configuration. |
| interface <i>interface-id</i> | (Optional) With mrouter , specify the next-hop interface to the multicast router. With static , specify the interface of the member port. It can be one of these values: <ul style="list-style-type: none"> • fastethernet <i>interface number</i>—a Fast Ethernet 802.3 interface. • gigabitethernet <i>interface number</i>—a Gigabit Ethernet 802.3z interface. • port-channel <i>interface number</i>—a channel interface. The range is 0 to 48. |
| learn | (Optional) With mrouter , specify the multicast router learning method. |
| cgmp | Set the switch to learn multicast router ports by snooping on Cisco Group Management Protocol (CGMP) packets. |
| pim-dvmrp | Set the switch to learn multicast router ports by snooping on IGMP queries and Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets. |
| static <i>ip-address</i> | (Optional) Add a Layer 2 port as a member of a multicast group with the specified group IP address. |



Note

Though visible in the command-line help string, the **source-only-learning** and **tcn** keywords are not supported.

Defaults

IGMP snooping is globally enabled on the switch.

IGMP snooping is enabled on VLAN interfaces.

IGMP immediate-leave processing is disabled.

The default learning method is **pim-dvmrp**—to snoop IGMP queries and PIM-DVMRP packets.

By default, there are no ports specified as members of a static multicast group.

By default, there are no multicast router ports.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | 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.

You should only configure the Immediate Leave feature when there is a maximum of one receiver on every port in the VLAN. The configuration is saved in NVRAM.

The Immediate Leave feature is supported only with IGMP Version 2 hosts.

The CGMP learn method is useful for reducing control traffic.

The **static** keyword is used for configuring the IGMP member ports statically.

The enabled configuration (globally or per VLAN), the learn method, and the static ports and groups are saved in NVRAM.

Examples

This example shows how to globally enable IGMP snooping:

```
Switch(config)# ip igmp snooping
```

This example shows how to globally disable IGMP snooping:

```
Switch(config)# no ip igmp snooping
```

This example shows how to enable IGMP snooping on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1
```

This example shows how to disable IGMP snooping on VLAN 1:

```
Switch(config)# no ip igmp snooping vlan 1
```

This example shows how to enable IGMP immediate-leave processing on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```


This example shows how to disable IGMP immediate-leave processing on VLAN 1:

```
Switch(config)# no ip igmp snooping vlan 1 immediate-leave
```

This example shows how to configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

This example shows how to specify the multicast router learning method as CGMP:

```
Switch(config)# no ip igmp snooping vlan 1 mrouter learn cgmp
```

You can verify your 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 the IGMP snooping router ports. |
| show ip igmp snooping groups | Displays IGMP snooping multicast information. |

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).

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 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 |
|-------------|------------------------------|
| 12.1(19)EA1 | 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.

Examples

This example shows how to disable report suppression:

```
Switch(config)# no ip igmp snooping report-suppression
```

This example shows how to enable report suppression:

```
Switch(config)# 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 | Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN. |
| | show ip igmp snooping | Displays the IGMP snooping configuration of the switch or the VLAN. |

ip source binding

Use the **ip source binding** global configuration command to configure static IP source bindings on the switch. Use the **no** form of this command to delete static bindings.

ip source binding *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

no source binding *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

This command is available only if your switch is running the enhanced multilayer image (EMI).

| Syntax Description | | |
|--------------------------------------|--|--|
| mac-address | | Specify a MAC address. |
| vlan <i>vlan-id</i> | | Specify a VLAN number. The range is from 1 to 4094. |
| <i>ip-address</i> | | Specify an IP address. |
| interface <i>interface-id</i> | | Specify an interface on which to add or delete an IP source binding. |

Defaults No IP source bindings are configured.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|------------|------------------------------|
| | 12.2(20)SE | This command was introduced. |

Usage Guidelines A static IP source binding entry has an IP address, its associated MAC address, and its associated VLAN number. The entry is based on the MAC address and the VLAN number. If you modify an entry by changing only the IP address, the switch updates the entry instead creating a new one.

Examples This example shows how to add a static IP source binding:

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet0/1
```

This example shows how to add a static binding and then modify the IP address for it:

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface
gigabitethernet0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet0/1
```

You can verify your settings by entering the **show ip source binding** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|--|--|
| | ip verify source | Enables IP source guard on an interface. |
| | show ip source binding | Displays the IP source bindings on the switch. |
| | show ip verify source | Displays the IP source guard configuration on the switch or on a specific interface. |

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 |
|-------------|------------------------------|
| 12.1(19)EA1 | 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 . |

ip verify source

Use the **ip verify source** interface configuration command to enable IP source guard on an interface. Use the **no** form of this command to disable IP source guard.

ip verify source [port-security]

no ip verify source

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|----------------------|---|
| port-security | (Optional) Enable IP source guard with IP and MAC address filtering. If you do not enter the port-security keyword, IP source guard with IP address filtering is enabled. |
|----------------------|---|

Defaults

IP source guard is disabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

To enable IP source guard with source IP and MAC address filtering, use the **ip verify source port-security** interface configuration command.

To enable IP source guard with source IP and MAC address filtering, you must enable port security on the interface.

Examples

This example shows how to enable IP source guard with source IP address filtering:

```
Switch(config-if)# ip verify source
```

This example shows how to enable IP source guard with source IP and MAC address filtering:

```
Switch(config-if)# ip verify source port-security
```

You can verify your settings by entering the **show ip source binding** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|---------------------------------------|--|
| | ip source binding | Configures static bindings on the switch. |
| | show ip verify source | Displays the IP source guard configuration on the switch or on a specific interface. |

l2protocol-tunnel

Use the **l2protocol-tunnel** interface configuration command to enable tunneling of Layer 2 protocols on an access port, 802.1Q tunnel port, or a port channel. You can enable tunneling for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. You can also enable point-to-point tunneling for Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or UniDirectional Link Detection (UDLD) packets. Use the **no** form of this command to disable tunneling on the interface.

```
l2protocol-tunnel [cdp | stp | vtp] [point-to-point [pagp | lacp | udld]] | [shutdown-threshold
[cdp | stp | vtp] [point-to-point [pagp | lacp | udld]]] value | [drop-threshold [cdp | stp | vtp]
[point-to-point [pagp | lacp | udld]]] value
```

```
no l2protocol-tunnel [cdp | stp | vtp] [point-to-point [pagp | lacp | udld]] | [shutdown-threshold
[cdp | stp | vtp] [point-to-point [pagp | lacp | udld]]] | [drop-threshold [cdp | stp | vtp]
[point-to-point [pagp | lacp | udld]]]
```

| Syntax Description | l2protocol-tunnel | Enable point-to-multipoint tunneling of CDP, STP, and VTP packets. |
|--------------------|---------------------------|---|
| | cdp | (Optional) Enable tunneling of CDP, specify a shutdown threshold for CDP, or specify a drop threshold for CDP. |
| | stp | (Optional) Enable tunneling of STP, specify a shutdown threshold for STP, or specify a drop threshold for STP. |
| | vtp | (Optional) Enable tunneling of VTP, specify a shutdown threshold for VTP, or specify a drop threshold for VTP. |
| | point-to-point | (Optional) Enable point-to-point tunneling of PAgP, LACP, and UDLD packets. |
| | pagp | (Optional) Enable point-to-point tunneling of PAgP, specify a shutdown threshold for PAgP, or specify a drop threshold for PAgP. |
| | lacp | (Optional) Enable point-to-point tunneling of LACP, specify a shutdown threshold for LACP, or specify a drop threshold for LACP. |
| | udld | (Optional) Enable point-to-point tunneling of UDLD, specify a shutdown threshold for UDLD, or specify a drop threshold for UDLD. |
| | shutdown-threshold | (Optional) Set a shutdown threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface is shut down. |
| | drop-threshold | (Optional) Set a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets. |
| | <i>value</i> | Specify a threshold in packets per second to be received for encapsulation before the interface shuts down, or specify the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold. |

Defaults

The default is that no Layer 2 protocol packets are tunneled.

The default is no shutdown threshold for the number of Layer 2 protocol packets.

The default is no drop threshold for the number of Layer 2 protocol packets.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(25)SE | This command was introduced. |

Usage Guidelines

You must enter this command, with or without protocol types, to tunnel Layer 2 packets.

If you enter this command for a port channel, all ports in the channel must have the same configuration.

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 information is propagated across the network to all customer locations. When protocol tunneling is enabled, protocol packets are encapsulated with a well-known Cisco multicast address for transmission across the network. When the packets reach their destination, the well-known MAC address is replaced by the Layer 2 protocol MAC address.

You can enable Layer 2 protocol tunneling for CDP, STP, and VTP individually or for all three protocols.

In a service-provider network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When protocol tunneling is enabled on the service-provider switch for PAgP or LACP, remote customer switches receive the protocol data units (PDUs) and can negotiate automatic creation of EtherChannels.

To enable tunneling of PAgP, LACP, and UDLD packets, you must have a point-to-point network topology. To decrease the link-down detection time, you should also enable UDLD on the interface when you enable tunneling of PAgP or LACP packets.

You can enable point-to-point protocol tunneling for PAgP, LACP, and UDLD individually or for all three protocols.

**Caution**

PAgP, LACP, and UDLD tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

Enter the **shutdown-threshold** keyword to control the number of protocol packets per second that are received on an interface before it shuts down. When no protocol option is specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold on the interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

When the shutdown threshold is reached, the interface is error-disabled. If you enable error recovery by entering the **errdisable recovery cause l2ptguard** global configuration command, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out. If the error recovery mechanism is not enabled for **l2ptguard**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

Enter the **drop-threshold** keyword to control the number of protocol packets per second that are received on an interface before it drops packets. When no protocol option is specified with a keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a shutdown threshold on the interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

When the drop threshold is reached, the interface drops Layer 2 protocol packets until the rate at which they are received is below the drop threshold.

The configuration is saved in NVRAM.

**Note**

For more information about Layer 2 protocol tunneling, see the software configuration guide for this release.

Examples

This example shows how to enable protocol tunneling for CDP packets and to configure the shutdown threshold as 50 packets per second:

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
```

This example shows how to enable protocol tunneling for STP packets and to configure the drop threshold as 400 packets per second:

```
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel drop-threshold stp 400
```

This example shows how to enable point-to-point protocol tunneling for PAgP and UDLD packets and to configure the PAgP drop threshold as 1000 packets per second:

```
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
```

Related Commands

| Command | Description |
|--|--|
| l2protocol-tunnel cos | Configures a class of service (CoS) value for all tunneled Layer 2 protocol packets. |
| show errdisable recovery | Displays errdisable recovery timer information. |
| show l2protocol-tunnel | Displays information about ports configured for Layer 2 protocol tunneling, including port, protocol, class of service (CoS), and threshold. |

l2protocol-tunnel cos

Use the **l2protocol-tunnel cos** global configuration command to configure class of service (CoS) value for all tunneled Layer 2 protocol packets. Use the **no** form of this command to return to the default setting.

l2protocol-tunnel cos *value*

no l2protocol-tunnel cos

Syntax Description

| | |
|--------------|---|
| <i>value</i> | Specify CoS priority value for tunneled Layer 2 protocol packets. If a CoS value is configured for data packets for the interface, the default is to use this CoS value. If no CoS value is configured for the interface, the default is 5. The range is 0 to 7, with 7 being the highest priority. |
|--------------|---|

Defaults

The default is to use the CoS value configured for data on the interface. If no CoS value is configured, the default is 5 for all tunneled Layer 2 protocol packets.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(25)SE | This command was introduced. |

Usage Guidelines

When enabled, the tunneled Layer 2 protocol packets use this CoS value.
The value is saved in NVRAM.

Examples

This example shows how to configure a Layer-2 protocol-tunnel CoS value of 7:

```
Switch(config)# l2protocol-tunnel cos 7
```

Related Commands

| Command | Description |
|--|--|
| show l2protocol-tunnel | Displays information about ports configured for Layer 2 protocol tunneling, including CoS. |

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

| | | |
|---------------------------|-----------------|--|
| Syntax Description | <i>priority</i> | Port priority for LACP. The range is 1 to 65535. |
|---------------------------|-----------------|--|

| | | |
|-----------------|-----------------------|--|
| Defaults | The default is 32768. | |
|-----------------|-----------------------|--|

| | | |
|----------------------|-------------------------|--|
| Command Modes | Interface configuration | |
|----------------------|-------------------------|--|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

This command takes effect only on EtherChannel ports that are already configured for LACP.

The software assigns to every link between systems that operate LACP a unique priority made up of the system priority, system ID, port priority, and the port number. In priority comparisons, numerically lower values have higher priority. The switch uses the priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Ports are considered for active use in aggregation in link-priority order starting with the port attached to the highest priority link. Each port is selected for active use if the preceding higher priority selections can also be maintained. Otherwise, the port is selected for standby mode. 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).

The lower the priority, the more likely that the port will be used for LACP transmission.

For information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Examples

This 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 | Description |
|---|--|
| channel-group | Assigns an Ethernet port to an EtherChannel group. |
| lacp system-priority | Configures the LACP system priority. |
| show lacp [<i>channel-group-number</i>] internal | 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

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 |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Although this is a global configuration command, the priority takes effect only on EtherChannels that have physical ports that are already configured for LACP.

The software assigns to every link between systems that operate LACP a unique priority made up of the system priority, system ID, port priority, and the port number. In priority comparisons, numerically lower values have higher priority. The switch uses the priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Ports are considered for active use in aggregation in link-priority order, starting with the port attached to the highest priority link. Each port is selected for active use if the preceding higher priority selections can also be maintained. Otherwise, the port is selected for standby mode. 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).

The lower the priority, the more likely that the port will be used for LACP transmission.

For more information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Examples

This 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 | 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. |

logging event power-inline-status

Use the **logging event power-inline-status** interface configuration command to enable the logging of Power over Ethernet (PoE) events. Use the **no** form of this command to disable the logging of PoE status events; however, the **no** form of this command does not disable PoE error events.

logging event power-inline-status

no logging event power-inline-status

Syntax Description

power-inline-status Enable the logging of PoE messages.

Defaults

Logging of PoE events is enabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The **power-inline-status** keyword is available only on PoE interfaces.

Examples

This example shows how to enable logging of PoE events on a port:

```
Switch(config-if)# interface fastethernet0/1
Switch(config-if)# logging event power-inline-status
Switch(config-if)#
```

Related Commands

| Command | Description |
|---|---|
| power inline | Configures the power management mode for the specified PoE port or for all PoE ports. |
| show controllers power inline | Displays the values in the registers of the specified PoE controller. |

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

| | |
|------------------------------|--|
| <i>filesystem:filename</i> | 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: |
| <i>max-file-size</i> | (Optional) Specify the maximum logging file size. The range is 4096 to 2147483647. |
| <i>min-file-size</i> | (Optional) Specify the minimum logging file size. The range is 1024 to 2147483647. |
| <i>severity-level-number</i> | (Optional) Specify the logging severity level. The range is 0 to 7. See the <i>type</i> option for the meaning of each level. |
| <i>type</i> | (Optional) Specify the logging type. These keywords are valid: <ul style="list-style-type: none"> • 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 is 2048 bytes; the maximum file size is 4096 bytes.
The default severity level is 7 (**debugging** messages and numerically lower levels).

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The log file is stored in ASCII text format in an internal buffer on the switch. You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. If the switch fails, the log is lost unless you had previously saved it to flash memory by using the **logging file flash:filename** global configuration command.

After saving the log to flash memory by using the **logging file flash:filename** global configuration command, you can use the **more flash:filename** privileged EXEC command to display its contents.

The command rejects the minimum file size if it is greater than the maximum file size minus 1024; the minimum file size then becomes the maximum file size minus 1024.

Specifying a *level* causes messages at that level and numerically lower levels to be displayed.

Examples

This example shows how to save informational log messages to a file in flash memory:

```
Switch(config)# logging file flash:logfile informational
```

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

Related Commands

| Command | Description |
|----------------------------|--|
| show running-config | Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands . |

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 | |
|--------------------|--|
| <i>name</i> | 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 configuration (Layer 2 interfaces only)

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines You can apply MAC ACLs only to ingress Layer 2 interfaces. You cannot apply MAC ACLs to Layer 3 interfaces.

On Layer 2 interfaces, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC access lists. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP ACL and a MAC ACL to the interface. You can apply no more than one IP access list and one MAC access list to the 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.

If you apply an ACL to a Layer 2 interface on a switch, and the switch has an input Layer 3 ACL or a VLAN map applied to a VLAN that the interface is a member of, the ACL applied to the Layer 2 interface takes precedence.

When an inbound packet is received on an interface with a MAC ACL applied, the switch checks the match conditions in the ACL. If the conditions are matched, the switch forwards or drops the packet, according to the ACL.

If the specified ACL does not exist, the switch forwards all packets.



Note

For more information about configuring MAC extended ACLs, see the “Configuring Network Security with ACLs” chapter 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 running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

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.



Note

You cannot apply named MAC extended ACLs to Layer 3 interfaces.

mac access-list extended *name*

no mac access-list extended *name*

Syntax Description

| | |
|-------------|--|
| <i>name</i> | 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 |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

MAC named extended lists are used with VLAN maps and class maps.

You can apply named MAC extended ACLs to VLAN maps or to Layer 2 interfaces; you cannot apply named MAC extended ACLs to Layer 3 interfaces.

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 \(ARP access-list configuration\)](#) command.



Note

For more information about MAC extended access lists, see the software configuration guide for this 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 (ARP 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 Description | | |
|----------------------------|--|---|
| 0 | | This value disables aging. Static address entries are never aged or removed from the table. |
| <i>10-1000000</i> | | Aging time in seconds. The range is 10 to 1000000 seconds. |
| vlan <i>vlan-id</i> | | (Optional) Specify the VLAN ID to which to apply the aging time. The range is 1 to 4094. |

Defaults The default is 300 seconds.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again. If you do not specify a specific VLAN, this command sets the aging time for all VLANs.

Examples This example shows how to set the aging time to 200 seconds for all VLANs:

```
Switch(config)# mac address-table aging-time 200
```

You can verify your setting by entering the **show mac address-table aging-time** privileged EXEC command.

■ mac address-table aging-time

| Related Commands | Command | Description |
|------------------|---|--|
| | show mac address-table aging-time | Displays the MAC address table aging time for all VLANs or the specified VLAN. |

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 <i>value</i> | (Optional) Configure the maximum number of entries in the MAC notification history table. The range is 1 to 500 entries. |
| interval <i>value</i> | (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 address notification feature is disabled.

The default trap interval value is 1 second.

The default number of entries in the history table is 1.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The MAC address notification feature sends Simple Network Management Protocol (SNMP) traps to the network management system (NMS) whenever a new MAC address is added or an old address is deleted from the forwarding tables. MAC notifications are generated only for dynamic and secure MAC addresses. Events are 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.

You enable the MAC address notification feature by using the **mac address-table notification** command. You must also enable MAC address notification traps on an interface by using the **snmp trap mac-notification** interface configuration command and configure the switch to send MAC address traps to the NMS by using the **snmp-server enable traps mac-notification** global configuration command.

Examples

This example shows how to enable the MAC address-table notification feature, set the interval time to 60 seconds, and set the history-size to 100 entries:

```
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
Switch(config)# mac address-table notification history-size 100
```

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

| Related Commands | 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

| | |
|--------------------------------------|--|
| <i>mac-addr</i> | 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 <i>vlan-id</i> | Specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094. |
| interface <i>interface-id</i> | <i>Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.</i> |

Defaults

No static addresses are configured.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Examples

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
```

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

Related Commands

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

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 <i>vlan-id</i> | Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. |

Defaults

Unicast MAC address filtering is disabled. The switch does not drop traffic for specific source or destination MAC addresses.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

For example, if you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** command, the switch drops packets with the specified MAC address as a source or destination.

If you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* command, the switch adds the MAC address as a static address.

Examples

This 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 drop
```

This 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. |
| <i>macro-name</i> | 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 |
|-------------|---|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(18)SE | The parameter value keywords were added. |

Usage Guidelines

You can use the **macro trace** *macro-name* 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** *macro-name* ? 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.

There are Cisco-default Smartports macros embedded in the switch software. You can display these macros and the commands they contain by using the **show parser macro** user EXEC command.

Follow these guidelines when you apply a Cisco-default Smartports macro on an interface:

- Display all macros on the switch by using the **show parser macro** user EXEC command. Display the contents of a specific macro by using the **show parser macro name** *macro-name* user EXEC command.
- Keywords that begin with \$ mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter** *value* keywords.

The Cisco-default macros use the \$ character to help identify required keywords. There is no restriction on using the \$ character to define keywords when you create a macro.

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** *interface-id* 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'
```

This example shows how to display the Cisco-default **cisco-desktop** macro and how to apply the macro and set the access VLAN ID to 25 on an interface:

```
Switch# show parser macro cisco-desktop
-----
Macro name : cisco-desktop
Macro type : default

# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

macro apply

```
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
-----
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

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 *text* Enter a description about the macros that are applied to the specified interface.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with an interface. When multiple macros are applied on a single interface, the description text will be from the last applied macro.

This example shows how to add a description to an interface:

```
Switch(config-if)# macro description duplex settings
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

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. |

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 | Use the trace keyword to apply a macro to a switch and to debug the macro. |
| <i>macro-name</i> | 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 no default setting.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

You can use the **macro trace macro-name** global configuration command to apply and to show the macros running on a switch 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 switch.

When creating a macro that requires the assignment of unique values, use the **parameter value** 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 macro-name ?** 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.

There are Cisco-default Smartports macros embedded in the switch software. You can display these macros and the commands they contain by using the **show parser macro** user EXEC command.

Follow these guidelines when you apply a Cisco-default Smartports macro on a switch:

- Display all macros on the switch by using the **show parser macro** user EXEC command. Display the contents of a specific macro by using the **show parser macro name** *macro-name* user EXEC command.
- Keywords that begin with \$ mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter** *value* keywords.

The Cisco-default macros use the \$ character to help identify required keywords. There is no restriction on using the \$ character to define keywords when you create a macro.

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 global macro-applied configuration on a switch only by entering the **no** version of each command contained 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 linkup'
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 *text* Enter a description about the macros that are applied to the switch.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro.

This example shows how to add a description to a switch:

```
Switch(config)# macro global description uddld aggressive mode enabled
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

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. |
| show parser 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

| | |
|-------------------|--------------------|
| <i>macro-name</i> | Name of the macro. |
|-------------------|--------------------|

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|--|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(20)SE | The help string # macro keywords was added. |

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. Enter **# macro keywords word** to define the keywords that are available for use with the macro. You can enter up to three help string keywords separated by a space. If you enter more than three macro keywords, only the first three are shown.

Macro names are case sensitive. For example, the commands **macro name Sample-Macro** and **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 using **interface interface-id**. This could cause commands that follow **exit**, **end**, or **interface interface-id** to execute in a different command mode.

The **no** form of this command only deletes the macro definition. It does not affect the configuration of those interfaces on which the macro is already applied. You can delete a macro-applied configuration on an interface by entering the **default interface interface-id** interface configuration command.

Alternatively, you can create an *anti-macro* for an existing macro that contains the **no** form of all the corresponding commands in the original macro. Then apply the anti-macro to the interface.

You can modify a macro by creating a new macro with the same name as the existing macro. The newly created macro overwrites the existing macro but does not affect the configuration of those interfaces on which the original 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 gi0/1
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 $MAX ?
WORD Value of second keyword to replace
```

Related Commands

| Command | Description |
|--|--|
| macro apply | Applies a macro on an interface or applies and traces a macro on an interface. |
| macro description | Adds a description about the macros that are applied to an interface. |
| macro global | Applies a macro on a switch or applies and traces a macro on a switch |
| macro global description | Adds a description about the macros that are applied to the switch. |
| 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. |
| <i>name</i> | Name of the access list to match packets against. |
| <i>number</i> | Number of the access list to match packets against. This option is not valid for MAC access lists. |

Defaults

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

You enter access-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.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC 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 *a12*.

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address a12
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 (class-map configuration)

Use the **match** class-map configuration command to define the match criteria to classify traffic. Use the **no** form of this command to remove the match criteria.

```
match {access-group acl-index-or-name | input-interface interface-id-list | ip dscp dscp-list | ip precedence ip-precedence-list}
```

```
no match {access-group acl-index-or-name | input-interface interface-id-list | ip dscp dscp-list | ip precedence ip-precedence-list}
```

| Syntax Description | | |
|--|--|--|
| access-group <i>acl-index-or-name</i> | | 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. |
| input-interface <i>interface-id-list</i> | | Specify the physical ports to which the interface-level class map in a hierarchical policy map applies. You can specify up to six entries in the list by specifying a port (counts as one entry), a list of ports separated by a space (each port counts as an entry), or a range of ports separated by a hyphen (counts as two entries). This keyword is available only in Cisco IOS Release 12.2(25)SE or later. |
| ip dscp <i>dscp-list</i> | | List of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly-used value. |
| ip precedence <i>ip-precedence-list</i> | | List of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly-used value. |

Defaults No match criteria are defined.

Command Modes Class-map configuration

| Command History | Release | Modification |
|-----------------|-------------|--|
| | 12.1(19)EA1 | This command was introduced. |
| | 12.2(25)SE | The input-interface <i>interface-id-list</i> keyword was added. |

Usage Guidelines The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-all** and **match-any** keywords are equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

In Cisco IOS Release 12.2(25)SE or later, use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

Examples

This example shows how to create a class map called *class2*, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

This example shows how to create a class map called *class3*, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using *acl1*:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet0/1 gigabitethernet0/2
Switch(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Switch(config)# class-map match-all class4
Switch(config-cmap)# match input-interface gigabitethernet0/1 - gigabitethernet0/5
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. |

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(18)SE | The default setting changed from <i>disabled</i> to <i>enabled</i> . |
| | 12.1(19)EA1 | 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.

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 cable type (straight-through or crossover) is incorrect.

Auto-MDIX is supported on all 10/100 and 10/100/1000-Mbps interfaces and on 10/100/1000BASE-T/TX small form-factor pluggable (SFP)-module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

In releases earlier than Cisco IOS Release 12.2(18)SE, the default setting is *disabled*.

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 |
|------------------|--|--|
| | <code>show controllers ethernet-controller interface-id phy</code> | Displays general information about internal registers of an interface, including the operational state of Auto-MDIX. |

mls qos

Use the **mls qos** global configuration command to enable quality of service (QoS) for the entire switch. When the **mls qos** command is entered, QoS is enabled with the default parameters on all ports in the system. Use the **no** form of this command to reset all the QoS-related statistics and to disable the QoS features for the entire switch.

mls qos

no mls qos

Syntax Description

This command has no arguments or keywords.

Defaults

QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

When QoS is enabled with the **mls qos** global configuration command and all other QoS settings are set to their defaults, traffic is classified as best effort (the DSCP and CoS value is set to 0) without any policing. No policy maps are configured. The default port trust state on all ports is untrusted. The default ingress and egress queue settings are in effect.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

QoS must be globally enabled to use QoS classification, policing, mark down or drop, queueing, and traffic shaping features. You can create a policy-map and attach it to a port before entering the **mls qos** command. However, until you enter the **mls qos** command, QoS processing is disabled.

Policy-maps and class-maps used to configure QoS are not deleted from the configuration by the **no mls qos** command, but entries corresponding to policy maps are removed from the switch hardware to save system resources. To re-enable QoS with the previous configurations, use the **mls qos** command.

Toggling the QoS status of the switch with this command modifies (reallocates) the sizes of the queues. During the queue size modification, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets for this queue.

Examples

This example shows how to enable QoS on the switch:

```
Switch(config)# mls qos
```

You can verify your settings by entering the **show mls qos** privileged EXEC command.

Related Commands

| Command | Description |
|------------------------------|---------------------------|
| show mls qos | Displays QoS information. |

mls qos aggregate-policer

Use the **mls qos aggregate-policer** global configuration command to define policer parameters, which can be shared by multiple classes within 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 delete an aggregate policer.

mls qos aggregate-policer *aggregate-policer-name* *rate-bps* *burst-byte* **exceed-action** { **drop** | **policed-dscp-transmit** }

no mls qos aggregate-policer *aggregate-policer-name*

| Syntax Description | | |
|--|---|--|
| <i>aggregate-policer-name</i> | Name of the aggregate policer referenced by the police aggregate policy-map class configuration command. | |
| <i>rate-bps</i> | Specify the average traffic rate in bits per second (bps). The range is 8000 to 1000000000. | |
| <i>burst-byte</i> | Specify the normal burst size in bytes. The range is 8000 to 1000000. | |
| exceed-action drop | When the specified rate is exceeded, specify that the switch drop the packet. | |
| exceed-action policed-dscp-transmit | When the specified rate is exceeded, specify that the switch change the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then send the packet. | |

Defaults No aggregate policers are defined.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines Define an aggregate policer if the policer is shared with multiple classes. Policers for a port cannot be shared with other policers for another port; traffic from two different ports cannot be aggregated for policing purposes.

The port ASIC device, which controls more than one physical port, supports 256 policers (255 policers plus 1 **no** policer). The maximum number of policers supported per port is 64. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port (there is no guarantee that a port will be assigned to any policer).

You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

You cannot delete an aggregate policer if it is being used in a policy map. You must first use the **no police aggregate** *aggregate-policer-name* policy-map class configuration command to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** *aggregate-policer-name* command.

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to define the aggregate policer parameters and how to apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

Related Commands

| Command | Description |
|--|--|
| police aggregate | Creates a policer that is shared by different classes. |
| show mls qos aggregate-policer | Displays the quality of service (QoS) aggregate policer configuration. |

mls qos cos

Use the **mls qos cos** interface configuration command to define the default class of service (CoS) value of a port or to assign the default CoS to all incoming packets on the port. Use the **no** form of this command to return to the default setting.

```
mls qos cos {default-cos | override}
```

```
no mls qos cos {default-cos | override}
```

Syntax Description

| | |
|--------------------|---|
| <i>default-cos</i> | Assign a default CoS value to a port. If packets are untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7. |
| override | Override the CoS of the incoming packets, and apply the default CoS value on the port to all incoming packets. |

Defaults

The default CoS value for a port is 0.
CoS override is disabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

You can use the default value to assign a CoS and Differentiated Services Code Point (DSCP) value to all incoming packets that are untagged (if the incoming packet does not have a CoS value). You also can assign a default CoS and DSCP value to all incoming packets by using the **override** keyword.

Use the **override** keyword when all incoming packets on certain ports deserve higher or lower priority than packets entering from other ports. Even if a port is previously set to trust DSCP, CoS, or IP precedence, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

Examples

This example shows how to configure the default port CoS to 4 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

This example shows how to assign all the packets entering a port to the default port CoS value of 4 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

| Command | Description |
|--|--|
| show mls qos interface | Displays quality of service (QoS) information. |

mls qos dscp-mutation

Use the **mls qos dscp-mutation** interface configuration command to apply a Differentiated Services Code Point (DSCP)-to-DSCP-mutation map to a DSCP-trusted port. Use the **no** form of this command to return the map to the default settings (no DSCP mutation).

mls qos dscp-mutation *dscp-mutation-name*

no mls qos dscp-mutation *dscp-mutation-name*

Syntax Description

| | |
|---------------------------|--|
| <i>dscp-mutation-name</i> | Name of the DSCP-to-DSCP-mutation map. This map was previously defined with the mls qos map dscp-mutation global configuration command. |
|---------------------------|--|

Defaults

The default DSCP-to-DSCP-mutation map is a null map, which maps incoming DSCPs to the same DSCP values.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

If two quality of service (QoS) domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate one set of DSCP values to match the definition of another domain. You apply the DSCP-to-DSCP-mutation map to the receiving port (ingress mutation) at the boundary of a quality of service (QoS) administrative domain.

With ingress mutation, the new DSCP value overwrites the one in the packet, and QoS handles the packet with this new value. The switch sends the packet out the port with the new DSCP value.

You can configure multiple DSCP-to-DSCP-mutation maps on ingress ports.

You apply the map only to DSCP-trusted ports. If you apply the DSCP mutation map to an untrusted port, to class of service (CoS) or IP-precedence trusted port, the command has no immediate effect until the port becomes DSCP-trusted.

Examples

This example shows how to define the DSCP-to-DSCP-mutation map named *dscpmutation1* and to apply the map to a port:

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

This example show how to remove the DSCP-to-DSCP-mutation map name *dscpmutation1* from the port and to reset the map to the default:

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|---|--|
| | mls qos map dscp-mutation | Defines the DSCP-to-DSCP-mutation map. |
| | mls qos trust | Configures the port trust state. |
| | show mls qos maps | Displays QoS mapping information. |

mls qos map

Use the **mls qos map** global configuration command to define the class of service (CoS)-to-Differentiated Services Code Point (DSCP) map, DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map. Use the **no** form of this command to return to the default map.

```
mls qos map { cos-dscp dscp1...dscp8 | dscp-cos dscp-list to cos | dscp-mutation
dscp-mutation-name in-dscp to out-dscp | ip-prec-dscp dscp1...dscp8 | policed-dscp dscp-list
to mark-down-dscp }
```

```
no mls qos map { cos-dscp | dscp-cos | dscp-mutation dscp-mutation-name | ip-prec-dscp |
policed-dscp }
```

Syntax Description

| | |
|--|---|
| cos-dscp <i>dscp1...dscp8</i> | Define the CoS-to-DSCP map. For <i>dscp1...dscp8</i> , enter eight DSCP values that correspond to CoS values 0 to 7. Separate each DSCP value with a space. The range is 0 to 63. |
| dscp-cos <i>dscp-list</i> to <i>cos</i> | Define the DSCP-to-CoS map. For <i>dscp-list</i> , enter up to eight DSCP values, with each value separated by a space. The range is 0 to 63. Then enter the to keyword. For <i>cos</i> , enter a single CoS value to which the DSCP values correspond. The range is 0 to 7. |
| dscp-mutation <i>dscp-mutation-name in-dscp</i> to <i>out-dscp</i> | Define the DSCP-to-DSCP-mutation map. For <i>dscp-mutation-name</i> , enter the mutation map name. For <i>in-dscp</i> , enter up to eight DSCP values, with each value separated by a space. Then enter the to keyword. For <i>out-dscp</i> , enter a single DSCP value. The range is 0 to 63. |
| ip-prec-dscp <i>dscp1...dscp8</i> | Define the IP-precedence-to-DSCP map. For <i>dscp1...dscp8</i> , enter eight DSCP values that correspond to the IP precedence values 0 to 7. Separate each DSCP value with a space. The range is 0 to 63. |
| policed-dscp <i>dscp-list</i> to <i>mark-down-dscp</i> | Define the policed-DSCP map. For <i>dscp-list</i> , enter up to eight DSCP values, with each value separated by a space. Then enter the to keyword. For <i>mark-down-dscp</i> , enter the corresponding policed (marked down) DSCP value. The range is 0 to 63. |

Defaults

Table 2-6 shows the default CoS-to-DSCP map:

Table 2-6 *Default CoS-to-DSCP Map*

| CoS Value | DSCP Value |
|-----------|------------|
| 0 | 0 |
| 1 | 8 |
| 2 | 16 |
| 3 | 24 |
| 4 | 32 |
| 5 | 40 |
| 6 | 48 |
| 7 | 56 |

Table 2-7 shows the default DSCP-to-CoS map:

Table 2-7 *Default DSCP-to-CoS Map*

| DSCP Value | CoS Value |
|------------|-----------|
| 0–7 | 0 |
| 8–15 | 1 |
| 16–23 | 2 |
| 24–31 | 3 |
| 32–39 | 4 |
| 40–47 | 5 |
| 48–55 | 6 |
| 56–63 | 7 |

Table 2-8 shows the default IP-precedence-to-DSCP map:

Table 2-8 *Default IP-Precedence-to-DSCP Map*

| IP Precedence Value | DSCP Value |
|---------------------|------------|
| 0 | 0 |
| 1 | 8 |
| 2 | 16 |
| 3 | 24 |
| 4 | 32 |
| 5 | 40 |
| 6 | 48 |
| 7 | 56 |

The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

All the maps are globally defined. All the maps, except the DSCP-to-DSCP-mutation map, are applied to all ports. The DSCP-to-DSCP-mutation map is applied to a specific port.

Examples

This example shows how to define the IP-precedence-to-DSCP map and to map IP-precedence values 0 to 7 to DSCP values of 0, 10, 20, 30, 40, 50, 55, and 60:

```
Switch# configure terminal
Switch(config)# mls qos map ip-prec-dscp 0 10 20 30 40 50 55 60
```

This example shows how to define the policed-DSCP map. DSCP values 1, 2, 3, 4, 5, and 6 are marked down to DSCP value 0. Marked DSCP values that not explicitly configured are not modified:

```
Switch# configure terminal
Switch(config)# mls qos map policed-dscp 1 2 3 4 5 6 to 0
```

This example shows how to define the DSCP-to-CoS map. DSCP values 20, 21, 22, 23, and 24 are mapped to CoS 1. DSCP values 10, 11, 12, 13, 14, 15, 16, and 17 are mapped to CoS 0:

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 20 21 22 23 24 to 1
Switch(config)# mls qos map dscp-cos 10 11 12 13 14 15 16 17 to 0
```

This example shows how to define the CoS-to-DSCP map. CoS values 0 to 7 are mapped to DSCP values 0, 5, 10, 15, 20, 25, 30, and 35:

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 0 5 10 15 20 25 30 35
```

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remain as specified in the null map):

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|---------------------------------------|---|
| | mls qos dscp-mutation | Applies a DSCP-to-DSCP-mutation map to a DSCP-trusted port. |
| | show mls qos maps | Displays quality of service (QoS) mapping information. |

mls qos queue-set output buffers

Use the **mls qos queue-set output buffers** global configuration command to allocate buffers to a queue-set (four egress queues per port). Use the **no** form of this command to return to the default setting.

mls qos queue-set output *qset-id* **buffers** *allocation1 ... allocation4*

no mls qos queue-set output *qset-id* **buffers**

Syntax Description

| | |
|------------------------------------|--|
| <i>qset-id</i> | ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2. |
| <i>allocation1 ... allocation4</i> | Buffer space allocation (percentage) for each queue (four values for queues 1 to 4). For <i>allocation1</i> , <i>allocation3</i> , and <i>allocation4</i> , the range is 0 to 99. For <i>allocation2</i> , the range is 1 to 100 (including the CPU buffer). Separate each value with a space. |

Defaults

All allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has 1/4 of the buffer space.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|---|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(20)SE | The range for <i>allocation1</i> , <i>allocation3</i> , and <i>allocation4</i> changed from 0 to 100 to 0 to 99. The range for <i>allocation2</i> changed from 20 to 100 to 1 to 100. |

Usage Guidelines

Specify four allocation values, and separate each with a space.

Allocate buffers according to the importance of the traffic; for example, give a large percentage of the buffer to the queue with the highest-priority traffic.

To configure different classes of traffic with different characteristics, use this command with the **mls qos queue-set output** *qset-id* **threshold** global configuration command.



Note

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Examples

This example shows how to map a port to queue-set 2. It allocates 40 percent of the buffer space to egress queue 1 and 20 percent to egress queues 2, 3, and 4:

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

| Command | Description |
|--|--|
| mls qos queue-set output threshold | Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set. |
| queue-set | Maps a port to a queue-set. |
| show mls qos interface buffers | Displays quality of service (QoS) information. |
| show mls qos queue-set | Displays egress queue settings for the queue-set. |

mls qos queue-set output threshold

Use the **mls qos queue-set output threshold** global configuration command to configure the weighted tail-drop (WTD) thresholds, to guarantee the availability of buffers, and to configure the maximum memory allocation to a queue-set (four egress queues per port). Use the **no** form of this command to return to the default setting.

mls qos queue-set output *qset-id* **threshold** *queue-id* *drop-threshold1* *drop-threshold2*
reserved-threshold *maximum-threshold*

no mls qos queue-set output *qset-id* **threshold** [*queue-id*]

| Syntax Description | | |
|--|--|--|
| <i>qset-id</i> | ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2. | |
| <i>queue-id</i> | Specific queue in the queue-set on which the command is performed. The range is 1 to 4. | |
| <i>drop-threshold1</i> <i>drop-threshold2</i> | Two WTD thresholds expressed as a percentage of the queue's allocated memory. The range is 1 to 400 percent. | |
| <i>reserved-threshold</i> | Amount of memory to be guaranteed (reserved) for the queue and expressed as a percentage of the allocated memory. The range is 1 to 100 percent. | |
| <i>maximum-threshold</i> | Enable a queue in the full condition to obtain more buffers than are reserved for it. This is the maximum memory the queue can have before the packets are dropped. The range is 1 to 400 percent. | |

Defaults

When quality of service (QoS) is enabled, WTD is enabled.

[Table 2-9](#) shows the default WTD threshold settings.

Table 2-9 Default Egress Queue WTD Threshold Settings

| Feature | Queue 1 | Queue 2 | Queue 3 | Queue 4 |
|----------------------|-------------|-------------|-------------|-------------|
| WTD Drop Threshold 1 | 100 percent | 50 percent | 100 percent | 100 percent |
| WTD Drop Threshold 2 | 100 percent | 50 percent | 100 percent | 100 percent |
| Reserved Threshold | 50 percent | 100 percent | 50 percent | 50 percent |
| Maximum Threshold | 400 percent | 400 percent | 400 percent | 400 percent |

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Use the **mls qos queue-set output *qset-id* buffers** global configuration command to allocate a fixed number of buffers to the four queues in a queue-set.

The drop-threshold percentages can exceed 100 percent and can be up to the maximum (if the maximum threshold exceeds 100 percent).

**Note**

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue, to prevent any queue or port from consuming all the buffers and depriving other queues, and to decide whether to grant buffer space to a requesting queue. The switch decides whether the target queue has not consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over-limit), and whether the common pool is empty (no free buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the reserved pool or from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

Examples

This example shows how to map a port to queue-set 2. It configures the drop thresholds for queue 2 to 40 and 60 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory this queue can have before packets are dropped:

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface [*interface-id*] buffers** or the **show mls qos queue-set** privileged EXEC command.

Related Commands

| Command | Description |
|---|---|
| mls qos queue-set output buffers | Allocates buffers to a queue-set. |
| queue-set | Maps a port to a queue-set. |
| show mls qos interface buffers | Displays QoS information. |
| show mls qos queue-set | Displays egress queue settings for the queue-set. |

mls qos rewrite ip dscp

Use the **mls qos rewrite ip dscp** global configuration command to configure the switch to change (rewrite) the Differentiated Services Code Point (DSCP) field of an incoming IP packet. Use the **no** form of this command to configure the switch to not modify (rewrite) the DSCP field of the packet and to enable DSCP transparency.

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

Syntax Description

This command has no arguments or keywords.

Defaults

DSCP transparency is disabled. The switch changes the DSCP field of the incoming IP packet.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(25)SE | This command was introduced. |

Usage Guidelines

DSCP transparency affects only the DSCP field of a packet at the egress. If DSCP transparency is enabled by using the **no mls qos rewrite ip dscp** command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.



Note

Enabling DSCP transparency does not affect the port trust settings on 802.1q tunneling ports.

By default, DSCP transparency is disabled. The switch modifies the DSCP field in an incoming packet, and the DSCP field in the outgoing packet is based on the quality of service (QoS) configuration, including the port trust setting, policing and marking, and the DSCP-to-DSCP mutation map.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet that the switch uses to generate a class of service (CoS) value representing the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

For example, if QoS is enabled and an incoming packet has a DSCP value of 32, the switch might modify the internal DSCP value based on the policy-map configuration and change the internal DSCP value to 16. If DSCP transparency is enabled, the outgoing DSCP value is 32 (same as the incoming value). If DSCP transparency is disabled, the outgoing DSCP value is 16 because it is based on the internal DSCP value.

Examples

This example shows how to enable DSCP transparency and configure the switch to not change the DSCP value of the incoming IP packet:

```
Switch(config)# mls qos
Switch(config)# no mls qos rewrite ip dscp
```

This example shows how to disable DSCP transparency and configure the switch to change the DSCP value of the incoming IP packet:

```
Switch(config)# mls qos
Switch(config)# mls qos rewrite ip dscp
```

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

Related Commands

| Command | Description |
|--|--|
| mls qos | Enables QoS globally. |
| show mls qos | Displays QoS information. |
| show running-config include rewrite | Displays the DSCP transparency setting. For syntax information, select Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

mls qos srr-queue input bandwidth

Use the **mls qos srr-queue input bandwidth** global configuration command to assign shaped round robin (SRR) weights to an ingress queue. The ratio of the weights is the ratio of the frequency in which the SRR scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue input bandwidth weight1 weight2
```

```
no mls qos srr-queue input bandwidth
```

Syntax Description

weight1 weight2 Ratio of *weight1* and *weight2* determines the ratio of the frequency in which the SRR scheduler dequeues packets from ingress queues 1 and 2. The range is 1 to 100. Separate each value with a space.

Defaults

Weight1 and weight2 are 4 (1/2 of the bandwidth is equally shared between the two queues).

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

SRR services the priority queue for its configured weight as specified by the **bandwidth** keyword in the **mls qos srr-queue input priority-queue *queue-id* bandwidth *weight*** global configuration command. Then SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the **mls qos srr-queue input bandwidth *weight1 weight2*** global configuration command.

You specify which ingress queue is the priority queue by using the **mls qos srr-queue input priority-queue** global configuration command.

Examples

This example shows how to assign the ingress bandwidth for the queues. Priority queueing is disabled, and the shared bandwidth ratio allocated to queue 1 is 25/(25+75) and to queue 2 is 75/(25+75):

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

In this example, queue 2 has three times the bandwidth of queue 1; queue 2 is serviced three times as often as queue 1.

This example shows how to assign the ingress bandwidths for the queues. Queue 1 is the priority queue with 10 percent of the bandwidth allocated to it. The bandwidth ratio allocated to queues 1 and 2 is 4/(4+4). SRR services queue 1 (the priority queue) first for its configured 10 percent bandwidth. Then SRR equally shares the remaining 90 percent of the bandwidth between queues 1 and 2 by allocating 45 percent to each queue:

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **queueing** or the **show mls qos input-queue** privileged EXEC command.

Related Commands

| Command | Description |
|---|---|
| mls qos srr-queue input buffers | Allocates the buffers between the ingress queues. |
| mls qos srr-queue input cos-map | Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID. |
| mls qos srr-queue input dscp-map | Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID. |
| mls qos srr-queue input priority-queue | Configures the ingress priority queue and guarantees bandwidth. |
| mls qos srr-queue input threshold | Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue. |
| show mls qos input-queue | Displays ingress queue settings. |
| show mls qos interface queueing | Displays quality of service (QoS) information. |

mls qos srr-queue input buffers

Use the **mls qos srr-queue input buffers** global configuration command to allocate the buffers between the ingress queues. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue input buffers percentage1 percentage2
```

```
no mls qos srr-queue input buffers
```

| | | |
|---------------------------|--|---|
| Syntax Description | <i>percentage1</i> <i>percentage2</i> | Percentage of buffers allocated to ingress queues 1 and 2. The range is 0 to 100. Separate each value with a space. |
|---------------------------|--|---|

| | |
|-----------------|---|
| Defaults | Ninety percent of the buffers is allocated to queue 1, and 10 percent of the buffers is allocated to queue 2. |
|-----------------|---|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | You should allocate the buffers so that the queues can handle any incoming bursty traffic. |
|-------------------------|--|

Examples This example shows how to allocate 60 percent of the buffer space to ingress queue 1 and 40 percent of the buffer space to ingress queue 2:

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

You can verify your settings by entering the **show mls qos interface [interface-id] buffers** or the **show mls qos input-queue** privileged EXEC command.

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

| Command | Description |
|---|--|
| <code>show mls qos input-queue</code> | Displays ingress queue settings. |
| <code>show mls qos interface buffers</code> | Displays quality of service (QoS) information. |

mls qos srr-queue input cos-map

Use the **mls qos srr-queue input cos-map** global configuration command to map class of service (CoS) values to an ingress queue or to map CoS values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue input cos-map queue queue-id {cos1...cos8 | threshold threshold-id
cos1...cos8}
```

```
no mls qos srr-queue input cos-map
```

Syntax Description

| | |
|--|--|
| queue <i>queue-id</i> | Specify a queue number. For <i>queue-id</i> , the range is 1 to 2. |
| <i>cos1...cos8</i> | Map CoS values to an ingress queue. For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7. |
| threshold <i>threshold-id</i> <i>cos1...cos8</i> | Map CoS values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7. |

Defaults

Table 2-10 shows the default CoS input queue threshold map:

Table 2-10 Default CoS Input Queue Threshold Map

| CoS Value | Queue ID - Threshold ID |
|-----------|-------------------------|
| 0–4 | 1–1 |
| 5 | 2–1 |
| 6, 7 | 1–1 |

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The CoS assigned at the ingress port selects an ingress or egress queue and threshold.

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state. You can assign two weighted tail-drop (WTD) threshold percentages to an ingress queue by using the **mls qos srr-queue input threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

Examples

This example shows how to map CoS values 0 to 3 to ingress queue 1 and to threshold ID 1 with a drop threshold of 50 percent. It maps CoS values 4 and 5 to ingress queue 1 and to threshold ID 2 with a drop threshold of 70 percent:

```
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 4 5
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| mls qos srr-queue input bandwidth | Assigns shaped round robin (SRR) weights to an ingress queue. |
| mls qos srr-queue input buffers | Allocates the buffers between the ingress queues. |
| mls qos srr-queue input dscp-map | Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID. |
| mls qos srr-queue input priority-queue | Configures the ingress priority queue and guarantees bandwidth. |
| mls qos srr-queue input threshold | Assigns WTD threshold percentages to an ingress queue. |
| show mls qos maps | Displays QoS mapping information. |

mls qos srr-queue input dscp-map

Use the **mls qos srr-queue input dscp-map** global configuration command to map Differentiated Services Code Point (DSCP) values to an ingress queue or to map DSCP values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue input dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id
dscp1...dscp8}
```

```
no mls qos srr-queue input dscp-map
```

Syntax Description

| | |
|--|--|
| queue <i>queue-id</i> | Specify a queue number. For <i>queue-id</i> , the range is 1 to 2. |
| <i>dscp1...dscp8</i> | Map DSCP values to an ingress queue. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63. |
| threshold <i>threshold-id</i> <i>dscp1...dscp8</i> | Map DSCP values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63. |

Defaults

Table 2-11 shows the default DSCP input queue threshold map:

Table 2-11 Default DSCP Input Queue Threshold Map

| DSCP Value | Queue ID–Threshold ID |
|------------|-----------------------|
| 0–39 | 1–1 |
| 40–47 | 2–1 |
| 48–63 | 1–1 |

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The DSCP assigned at the ingress port selects an ingress or egress queue and threshold.

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state. You can assign two weighted tail-drop (WTD) threshold percentages to an ingress queue by using the **mls qos srr-queue input threshold** global configuration command.

You can map each DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

Examples

This example shows how to map DSCP values 0 to 6 to ingress queue 1 and to threshold 1 with a drop threshold of 50 percent. It maps DSCP values 20 to 26 to ingress queue 1 and to threshold 2 with a drop threshold of 70 percent:

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| mls qos srr-queue input bandwidth | Assigns shaped round robin (SRR) weights to an ingress queue. |
| mls qos srr-queue input buffers | Allocates the buffers between the ingress queues. |
| mls qos srr-queue input cos-map | Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to threshold ID. |
| mls qos srr-queue input priority-queue | Configures the ingress priority queue and guarantees bandwidth. |
| mls qos srr-queue input threshold | Assigns WTD threshold percentages to an ingress queue. |
| show mls qos maps | Displays QoS mapping information. |

mls qos srr-queue input priority-queue

Use the **mls qos srr-queue input priority-queue** global configuration command to configure the ingress priority queue and to guarantee bandwidth on the internal ring if the ring is congested. Use the **no** form of this command to return to the default setting.

mls qos srr-queue input priority-queue *queue-id* **bandwidth** *weight*

no mls qos srr-queue input priority-queue *queue-id*

Syntax Description

| | |
|--------------------------------|--|
| <i>queue-id</i> | Ingress queue ID. The range is 1 to 2. |
| bandwidth <i>weight</i> | Bandwidth percentage of the internal ring. The range is 0 to 40. |

Defaults

The priority queue is queue 2, and 10 percent of the bandwidth is allocated to it.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

You should use the priority queue only for traffic that needs to be expedited (for example, voice traffic, which needs minimum delay and jitter).

The priority queue is guaranteed part of the bandwidth on the internal ring, which reduces the delay and jitter under heavy network traffic on an oversubscribed ring (when there is more traffic than the backplane can carry, and the queues are full and dropping frames).

Shaped round robin (SRR) services the priority queue for its configured weight as specified by the **bandwidth** keyword in the **mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* global configuration command. Then SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the **mls qos srr-queue input bandwidth** *weight1* *weight2* global configuration command.

To disable priority queueing, set the bandwidth weight to 0, for example, **mls qos srr-queue input priority-queue** *queue-id* **bandwidth 0**.

Examples

This example shows how to assign the ingress bandwidths for the queues. Queue 1 is the priority queue with 10 percent of the bandwidth allocated to it. The bandwidth ratio allocated to queues 1 and 2 is 4/(4+4). SRR services queue 1 (the priority queue) first for its configured 10 percent bandwidth. Then SRR equally shares the remaining 90 percent of the bandwidth between queues 1 and 2 by allocating 45 percent to each queue:

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

You can verify your settings by entering the **show mls qos interface** *[interface-id]* **queueing** or the **show mls qos input-queue** privileged EXEC command.

Related Commands

| Command | Description |
|---|---|
| mls qos srr-queue input bandwidth | Assigns shaped round robin (SRR) weights to an ingress queue. |
| mls qos srr-queue input buffers | Allocates the buffers between the ingress queues. |
| mls qos srr-queue input cos-map | Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID. |
| mls qos srr-queue input dscp-map | Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID. |
| mls qos srr-queue input threshold | Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue. |
| show mls qos input-queue | Displays ingress queue settings. |
| show mls qos interface queueing | Displays quality of service (QoS) information. |

mls qos srr-queue input threshold

Use the **mls qos srr-queue input threshold** global configuration command to assign weighted tail-drop (WTD) threshold percentages to an ingress queue. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2
```

```
no mls qos srr-queue input threshold queue-id
```

Syntax Description

| | |
|--|--|
| <i>queue-id</i> | ID of the ingress queue. The range is 1 to 2. |
| <i>threshold-percentage1</i> <i>threshold-percentage2</i> | Two WTD threshold percentage values. Each threshold value is a percentage of the total number of queue descriptors allocated for the queue. Separate each value with a space. The range is 1 to 100. |

Defaults

When quality of service (QoS) is enabled, WTD is enabled.

The two WTD thresholds are set to 100 percent.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

QoS uses the CoS-to-threshold map or the DSCP-to-threshold map to decide which class of service (CoS) or Differentiated Services Code Points (DSCPs) values are mapped to threshold 1 and to threshold 2. If threshold 1 is exceeded, packets with CoS or DSCPs assigned to this threshold are dropped until the threshold is no longer exceeded. However, packets assigned to threshold 2 continue to be queued and sent as long as the second threshold is not exceeded.

Each queue has two configurable (explicit) drop threshold and one preset (implicit) drop threshold (full).

You configure the CoS-to-threshold map by using the **mls qos srr-queue input cos-map** global configuration command. You configure the DSCP-to-threshold map by using the **mls qos srr-queue input dscp-map** global configuration command.

Examples

This example shows how to configure the tail-drop thresholds for the two queues. The queue 1 thresholds are 50 percent and 100 percent, and the queue 2 thresholds are 70 percent and 100 percent:

```
Switch(config)# mls qos srr-queue input threshold 1 50 100
Switch(config)# mls qos srr-queue input threshold 2 70 100
```

You can verify your settings by entering the **show mls qos interface** [*interface-id*] **buffers** or the **show mls qos input-queue** privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| mls qos srr-queue input bandwidth | Assigns shaped round robin (SRR) weights to an ingress queue. |
| mls qos srr-queue input buffers | Allocates the buffers between the ingress queues. |
| mls qos srr-queue input cos-map | Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID. |
| mls qos srr-queue input dscp-map | Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID. |
| mls qos srr-queue input priority-queue | Configures the ingress priority queue and guarantees bandwidth. |
| show mls qos input-queue | Displays ingress queue settings. |
| show mls qos interface buffers | Displays quality of service (QoS) information. |

mls qos srr-queue output cos-map

Use the **mls qos srr-queue output cos-map** global configuration command to map class of service (CoS) values to an egress queue or to map CoS values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue output cos-map queue queue-id {cos1...cos8 | threshold threshold-id
cos1...cos8}
```

```
no mls qos srr-queue output cos-map
```

Syntax Description

| | |
|--|--|
| queue <i>queue-id</i> | Specify a queue number. For <i>queue-id</i> , the range is 1 to 4. |
| <i>cos1...cos8</i> | Map CoS values to an egress queue. For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7. |
| threshold <i>threshold-id</i> <i>cos1...cos8</i> | Map CoS values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7. |

Defaults

Table 2-12 shows the default CoS output queue threshold map:

Table 2-12 Default Cos Output Queue Threshold Map

| CoS Value | Queue ID–Threshold ID |
|-----------|-----------------------|
| 0, 1 | 2–1 |
| 2, 3 | 3–1 |
| 4 | 4–1 |
| 5 | 1–1 |
| 6, 7 | 4–1 |

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

**Note**

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output *qset-id* threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

Examples

This example shows how to map a port to queue-set 1. It maps CoS values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface [*interface-id*] buffers**, or the **show mls qos queue-set** privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| mls qos srr-queue output dscp-map | Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID. |
| mls qos queue-set output threshold | Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set. |
| queue-set | Maps a port to a queue-set. |
| show mls qos interface buffers | Displays QoS information. |
| show mls qos maps | Displays QoS mapping information. |
| show mls qos queue-set | Displays egress queue settings for the queue-set. |

mls qos srr-queue output dscp-map

Use the **mls qos srr-queue output dscp-map** global configuration command to map Differentiated Services Code Point (DSCP) values to an egress or to map DSCP values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id
dscp1...dscp8}
```

```
no mls qos srr-queue output dscp-map
```

Syntax Description

| | |
|--|--|
| queue <i>queue-id</i> | Specify a queue number. For <i>queue-id</i> , the range is 1 to 4. |
| <i>dscp1...dscp8</i> | Map DSCP values to an egress queue. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63. |
| threshold <i>threshold-id</i> <i>dscp1...dscp8</i> | Map DSCP values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63. |

Defaults

Table 2-13 shows the default DSCP output queue threshold map:

Table 2-13 Default DSCP Output Queue Threshold Map

| DSCP Value | Queue ID–Threshold ID |
|------------|-----------------------|
| 0–15 | 2–1 |
| 16–31 | 3–1 |
| 32–39 | 4–1 |
| 40–47 | 1–1 |
| 48–63 | 4–1 |

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

**Note**

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output *qset-id* threshold** global configuration command.

You can map each DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

Examples

This example shows how to map a port to queue-set 1. It maps DSCP values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface *[interface-id]* buffers**, or the **show mls qos queue-set** privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| mls qos srr-queue output cos-map | Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID. |
| mls qos queue-set output threshold | Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set. |
| queue-set | Maps a port to a queue-set. |
| show mls qos interface buffers | Displays quality of service (QoS) information. |
| show mls qos maps | Displays QoS mapping information. |
| show mls qos queue-set | Displays egress queue settings for the queue-set. |

mls qos trust

Use the **mls qos trust** interface configuration command to configure the port trust state. Ingress traffic can be trusted, and classification is performed by examining the packet Differentiated Services Code Point (DSCP), class of service (CoS), or IP-precedence field. Use the **no** form of this command to return a port to its untrusted state.

mls qos trust [cos | device cisco-phone | dscp | ip-precedence]

no mls qos trust [cos | device | dscp | ip-precedence]

Syntax Description

| | |
|---------------------------|---|
| cos | (Optional) Classify an ingress packet by using the packet CoS value. For an untagged packet, use the port default CoS value. |
| device cisco-phone | (Optional) Classify an ingress packet by trusting the CoS or DSCP value sent from the Cisco IP Phone (trusted boundary), depending on the trust setting. |
| dscp | (Optional) Classify an ingress packet by using the packet DSCP value (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the default port CoS value is used. |
| ip-precedence | (Optional) Classify an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the port default CoS value is used. |

Defaults

The port is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|--|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(20)SE | The usage guidelines were revised to describe how the switch sets the trust state when a Cisco IP Phone is connected to a switch or routed port. |

Usage Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain. Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When a port is configured with trust DSCP or trust IP precedence and the incoming packet is a non-IP packet, the CoS-to-DSCP map is used to derive the corresponding DSCP value from the CoS value. The CoS can be the packet CoS for trunk ports or the port default CoS for nontrunk ports.

If the DSCP is trusted, the DSCP field of the IP packet is not modified. However, it is still possible that the CoS value of the packet is modified (according to DSCP-to-CoS map).

If the CoS is trusted, the CoS field of the packet is not modified, but the DSCP can be modified (according to CoS-to-DSCP map) if the packet is an IP packet.

The trusted boundary feature prevents security problems if users disconnect their PCs from networked Cisco IP Phones and connect them to the switch port to take advantage of trusted CoS or DSCP settings. You must globally enable the Cisco Discovery Protocol (CDP) on the switch and on the port connected to the IP phone. If the telephone is not detected, trusted boundary disables the trusted setting on the switch or routed port and prevents misuse of a high-priority queue.

If you configure the trust setting for DSCP or IP precedence, the DSCP or IP precedence values in the incoming packets are trusted. If you configure the **mls qos cos override** interface configuration command on the switch port connected to the IP phone, the switch overrides the CoS of the incoming voice and data packets and assigns the default CoS value to them.

For an inter-QoS domain boundary, you can configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different between the QoS domains.

Classification using a port trust state (for example, **mls qos trust [cos | dscp | ip-precedence]** and a policy map (for example, **service-policy input policy-map-name**) are mutually exclusive. The last one configured overwrites the previous configuration.

Examples

This example shows how to configure a port to trust the IP precedence field in the incoming packet:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust ip-precedence
```

This example shows how to specify that the Cisco IP Phone connected on a port is a trusted device:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust device cisco-phone
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

| Command | Description |
|-------------------------------|---|
| mls qos cos | Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port. |
| mls qos dscp-mutation | Applies a DSCP-to DSCP-mutation map to a DSCP-trusted port. |
| mls qos map | Defines the CoS-to-DSCP map, DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map. |
| show mls qos interface | Displays QoS information. |

mls qos vlan-based

Use the **mls qos vlan-based** interface configuration command to enable VLAN-based quality of service (QoS) on the physical port. Use the **no** form of this command to disable this feature.

mls qos vlan-based

no mls qos vlan-based

Syntax Description There are no arguments or keywords.

Defaults VLAN-based QoS is disabled.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|------------|------------------------------|
| | 12.2(25)SE | This command was introduced. |

Usage Guidelines Before attaching a hierarchical policy map to a switch virtual interface (SVI), use the **mls qos vlan-based** interface configuration command on a physical port if the port is to be specified in the secondary interface level of the hierarchical policy map.

When you configure hierarchical policing, the hierarchical policy map is attached to the SVI and affects all traffic belonging to the VLAN. The individual policer in the interface-level traffic classification only affects the physical ports specified for that classification.

For detailed instructions about configuring hierarchical policy maps, see the “Classifying, Policing, and Marking Traffic by Using Hierarchical Policy Maps” section in the software configuration guide for this release.

Examples This example shows how to enable VLAN-based policing on a physical port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos vlan-based
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|--|---------------------------|
| | show mls qos interface | Displays QoS information. |

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 ingress 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 replicate** keywords are ignored with the **no** form of the command.

```
monitor session session_number destination {interface interface-id [, | -] [encapsulation replicate] [ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | 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 replicate] [ingress {dot1q vlan vlan-id | isl | untagged vlan vlan-id | 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

| | |
|--------------------------------------|---|
| <i>session_number</i> | Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 66. |
| destination | Specify the SPAN or RSPAN destination. A destination must be a physical port. |
| 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. |
| encapsulation replicate | (Optional) Specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). 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 <i>vlan-id</i> | Specify ingress forwarding using 802.1Q encapsulation with the specified VLAN as the default VLAN for ingress traffic. |
| isl | Specify ingress forwarding using ISL encapsulation. |

| | |
|-------------------------------------|---|
| untagged vlan <i>vlan-id</i> | Specify ingress forwarding using untagged encapsulation with the specified VLAN as the default VLAN for ingress traffic |
| vlan <i>vlan-id</i> | When used with only the ingress keyword, set default VLAN for ingress traffic. |
| remote vlan <i>vlan-id</i> | 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 <i>vlan-id</i> | 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 <i>vlan-id</i> | 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 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 |
|-------------|------------------------------|
| 12.1(19)EA1 | 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 802.1x on a port that is a SPAN or RSPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination. (If 802.1x is not available on the port, the switch returns an error message.) You can enable 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**, **isl**, or **untagged**. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **ingress**, egress encapsulation is untagged; ingress encapsulation depends on the keywords that follow—**dot1q**, **isl**, 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:

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Switch(config)# no monitor session 2 destination gigabitethernet0/2
```

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 304
```

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.

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses 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.

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress untagged vlan 5
```

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 current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

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 <i>ip-address</i> | 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. |
| <i>count</i> | (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 <i>value</i> | (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 <i>vlan-id</i> | (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 |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

A maximum of 256 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 querytime** command applies only to receiver ports.

If the switch MVR is interoperating with Catalyst 2900 XL or Catalyst 3500 XL switches, set the multicast mode to compatible.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports. MVR can coexist with IGMP snooping on a switch.

Multicast routing and MVR cannot coexist on a switch. If you enable multicast routing and a multicast routing protocol while MVR is enabled, MVR is disabled and a warning message appears. If you try to enable MVR while multicast routing and a multicast routing protocol are enabled, the operation to enable MVR is cancelled with an Error message.

Examples This example shows how to enable MVR:

```
Switch(config)# mvr
```

This example shows how to disable MVR:

```
Switch(config)# no mvr
```

Use the **show mvr** privileged EXEC command to display the current setting for maximum multicast groups.

This example shows how to configure 228.1.23.4 as an IP multicast address:

```
Switch(config)# mvr group 228.1.23.4
```

This example shows how to configure ten contiguous IP multicast groups with multicast addresses from 228.1.23.1 to 228.1.23.10:

```
Switch(config)# mvr group 228.1.23.1 10
```

This example shows how to delete the previously configured ten IP multicast addresses:

```
Switch(config)# no mvr group 228.1.23.1 10
```

This example shows how to delete all previously configured IP multicast addresses:

```
Switch(config)# no mvr group
```

Use the **show mvr members** privileged EXEC command to display the IP multicast group addresses configured on the switch.

This example shows how to set the maximum query response time as one second (10 tenths):

```
Switch(config)# mvr querytime 10
```

This example shows how to return the maximum query response time to the default setting of one-half second:

```
Switch(config)# no mvr querytime
```

This example shows how to set VLAN 2 as the multicast VLAN:

```
Switch(config)# mvr vlan 2
```

You can verify your 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, status, and Immediate Leave configuration. 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]]
```

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

| Syntax Description | | |
|----------------------------------|---|--|
| immediate | (Optional) Enable the Immediate Leave feature of MVR on a port. Use the no mvr immediate command to disable the feature. | |
| type | (Optional) Configure the port as an MVR receiver port or a source port. 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. | |
| vlan <i>vlan-id</i> group | (Optional) Add the port as a static member of the multicast group with the specified VLAN ID. The no mvr vlan <i>vlan-id</i> group command removes a port on a VLAN from membership in an IP multicast address group. | |
| <i>ip-address</i> | (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 is joining. | |

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 |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

Configure a port as a source port if that port should be able to both send and receive multicast data bound for the configured multicast groups. Multicast data is received on all ports configured as source ports.

Receiver ports cannot be trunk ports. Receiver ports on 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 compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

An MVR port cannot be a private-VLAN port.

Examples

This example shows how to configure a port as an MVR receiver port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr type receiver
```

This example shows how to configure a port as an MVR source port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr type source
```

This example shows how to remove a port as an MVR port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no mvr
```

This example shows how to display configured receiver ports and source ports.

```
Switch# show mvr interface
Port      Type      Status      Immediate Leave
----      -
Gi0/1     SOURCE    ACTIVE/UP   DISABLED
Gi0/2     RECEIVER  ACTIVE/DOWN DISABLED
```

This example shows how to enable Immediate Leave on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr immediate
```

This example shows how to disable Immediate Leave on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no mvr immediate
```

This example shows how to add a port on VLAN 1 as a static member of IP multicast group 228.1.23.4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

This example shows how to remove this port from membership:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no mvr vlan5 group 228.1.23.4
```

This example shows how to remove this port from all IP multicast groups:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no mvr vlan5 group
```

This example shows the result if a port is not a receiver port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan 1 group 230.1.23.4
Interface Gi0/2 not configured as a receiver interface
```

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

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-port (logical port channel).

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The learn method must be configured the same at both ends of the link.



Note

The Catalyst 3560 switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAGP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the Catalyst 3560 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 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 channel-group-number internal** privileged EXEC command.

Related Commands

| Command | Description |
|------------------------------------|--|
| pagp port-priority | Selects a port over which all traffic through the EtherChannel is sent. |
| show pagp | Displays PAgP channel-group information. |
| show running-config | Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

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

Syntax Description

priority A priority number ranging from 0 to 255.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.



Note

The Catalyst 3560 switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the Catalyst 3560 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 current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

permit (ARP access-list configuration)

Use the **permit** Address Resolution Protocol (ARP) access-list configuration command to permit an ARP packet based on matches against the Dynamic Host Configuration Protocol (DHCP) bindings. Use the **no** form of this command to remove the specified access control entry (ACE) from the access control list.

```
permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

```
no permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

This command is available only if your switch is running the enhanced multilayer image (EMI).

| Syntax Description | |
|---|--|
| request | (Optional) Requests a match for the ARP request. When request is not specified, matching is performed against all ARP packets. |
| ip | Specify the sender IP address. |
| any | Accept any IP or MAC address. |
| host <i>sender-ip</i> | Accept the specified sender IP address. |
| <i>sender-ip</i> <i>sender-ip-mask</i> | Accept the specified range of sender IP addresses. |
| mac | Specify the sender MAC address. |
| host <i>sender-mac</i> | Accept the specified sender MAC address. |
| <i>sender-mac</i> <i>sender-mac-mask</i> | Accept the specified range of sender MAC addresses. |
| response ip | Define the IP address values for the ARP responses. |
| host <i>target-ip</i> | (Optional) Accept the specified target IP address. |
| <i>target-ip target-ip-mask</i> | (Optional) Accept the specified range of target IP addresses. |
| mac | Specify the MAC address values for the ARP responses. |
| host <i>target-mac</i> | (Optional) Accept the specified target MAC address. |
| <i>target-mac</i> <i>target-mac-mask</i> | (Optional) Accept the specified range of target MAC addresses. |
| log | (Optional) Log a packet when it matches the ACE. Matches are logged if you also configure the matchlog keyword in the ip arp inspection vlan logging global configuration command. |

Defaults

There are no default settings.

Command Modes

ARP access-list configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

You can add permit clauses to forward ARP packets based on some matching criteria.

Examples

This example shows how to define an ARP access list and to permit both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

Related Commands

| Command | Description |
|--|---|
| arp access-list | Defines an ARP access control list (ACL). |
| deny (ARP access-list configuration) | Denies an ARP packet based on matches against the DHCP bindings. |
| ip arp inspection filter vlan | Permits ARP requests and responses from a host configured with a static IP address. |
| show arp access-list | Displays detailed information about ARP access lists. |

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 | lavr-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 | lavr-sca | lsap lsap mask | mop-console |
mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```



Note

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 <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 mask</i> | 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. |
| <i>type mask</i> | (Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. <ul style="list-style-type: none"> <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 <i>cos</i> | (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. |
| lavr-sca | (Optional) Select EtherType DEC-LAVC-SCA. |

| | |
|-------------------------------------|--|
| lsap <i>lsap-number mask</i> | (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 2-14](#).

Table 2-14 IPX Filtering Criteria

| IPX Encapsulation Type | | Filter Criterion |
|------------------------|----------------|------------------|
| Cisco IOS Name | Novell Name | |
| 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 |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

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 name 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 name 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. |
| mac access-list extended | Creates an access list based on MAC addresses for non-IP traffic. |
| show access-lists | Displays access control lists configured on a switch. |

police

Use the **police** policy-map class configuration command to define a policer for classified traffic. 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 an existing policer.

```
police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]
```

```
no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]
```

| Syntax Description | | |
|--|------------|---|
| <i>rate-bps</i> | | Specify the average traffic rate in bits per second (bps). The range is 8000 to 1000000000. |
| <i>burst-byte</i> | | Specify the normal burst size in bytes. The range is 8000 to 1000000. |
| exceed-action drop | (Optional) | When the specified rate is exceeded, specify that the switch drop the packet. |
| exceed-action policed-dscp-transmit | (Optional) | When the specified rate is exceeded, specify that the switch changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet. |

Defaults No policers are defined.

Command Modes Policy-map class configuration

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines In Cisco IOS Release 12.2(25)SE or later, when configuring hierarchical policy maps, you can only use the **police** policy-map command in a secondary interface-level policy map.

The port ASIC device, which controls more than one physical port, supports 256 policers (255 policers plus 1 **no** policer). The maximum number of policers supported per port is 64. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

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

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how quickly (the average rate) the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

Examples

This example shows how to configure a policer that drops packets if traffic exceeds 1 Mbps average rate with a burst size of 20 KB. The DSCPs of incoming packets are trusted, and there is no packet modification.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action drop
Switch(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
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 (through the police , set , and trust policy-map class configuration commands) for the specified class-map name. |
| mls qos map policed-dscp | Applies a policed-DSCP map to a DSCP-trusted port. |
| policy-map | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| set | Classifies IP traffic by setting a DSCP or IP-precedence value in the packet. |
| show policy-map | Displays quality of service (QoS) policy maps. |
| trust | Defines a trust state for traffic classified through the class policy-map configuration or the class-map global configuration command. |

police aggregate

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 | |
|--------------------|--|
| | <i>aggregate-policer-name</i> Name of the aggregate policer. |

| Defaults | |
|----------|------------------------------------|
| | No aggregate policers are defined. |

| Command Modes | |
|---------------|--------------------------------|
| | Policy-map class configuration |

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

| Usage Guidelines | |
|------------------|--|
| | The port ASIC device, which controls more than one physical port, supports 256 policers (255 policers plus 1 no policer). The maximum number of policers supported per port is 64. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer. |

You set aggregate policer parameters by using the **mls qos aggregate-policer** global configuration command. You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

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

In Cisco IOS Release 12.2(25)SE or later, you cannot configure aggregate policers in hierarchical policy maps.

| Examples | |
|----------|---|
| | This example shows how to define the aggregate policer parameters and to apply the policer to multiple classes in a policy map: |

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
```

■ police aggregate

```
Switch(config-pmap) # class class3
Switch(config-pmap-c) # trust dscp
Switch(config-pmap-c) # police aggregate agg_policer2
Switch(config-pmap-c) # exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|--|--|
| | mls qos aggregate-policer | Defines policer parameters, which can be shared by multiple classes within a policy map. |
| | show mls qos aggregate-policer | Displays the quality of service (QoS) aggregate policer configuration. |

policy-map

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

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

| | |
|------------------------|-------------------------|
| <i>policy-map-name</i> | Name of the policy map. |
|------------------------|-------------------------|

Defaults

No policy maps are defined.

The default behavior is to set the Differentiated Services Code Point (DSCP) to 0 if the packet is an IP packet and to set the class of service (CoS) to 0 if the packet is tagged. No policing is performed.

Command Modes

Global configuration

Command History

| Release | Modification |
|-------------|--|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(25)SE | Support for policy maps on SVIs was added. |

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**: defines the classification match criteria for the specified class map. For more information, see the “[class](#)” section on page 2-33.
- **description**: describes the policy map (up to 200 characters).
- **exit**: exits policy-map configuration mode and returns you to global configuration mode.
- **no**: removes a previously defined policy map.
- **rename**: renames the current policy map.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

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, added to, 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.

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.

Only one policy map per ingress port or SVI is supported. You can apply the same policy map to multiple physical ports or SVIs.

In software releases earlier than Cisco IOS Release 12.2(25)SE, you can apply a policy map and configure policing only on physical ports. You can configure the trust state, set a new DSCP or IP precedence value in the packet, or define an individual or aggregate policer. For more information, see the “Policing on Physical Ports” section in the “Configuring QoS” chapter of the software configuration guide for this release.

In Cisco IOS Release 12.2(25)SE or later, you can apply a nonhierarchical policy maps to physical ports or to SVIs. A nonhierarchical policy map is the same as a port-based policy maps in software releases earlier than Cisco IOS Release 12.2(25)SE. However, a hierarchical policy map can only be applied to SVIs.

A hierarchical policy map has two levels. The first level, the VLAN level, specifies the actions to be taken against a traffic flow on an SVI. The second level, the interface level, specifies the actions to be taken against the traffic on the physical ports that belong to the SVI and are specified in the interface-level policy map.

In a primary VLAN-level policy map, you can only configure the trust state or set a new DSCP or IP precedence value in the packet. In a secondary interface-level policy map, you can only configure individual policers on physical ports that belong to the SVI.

After the hierarchical policy map is attached to an SVI, an interface-level policy map cannot be modified or removed from the hierarchical policy map. A new interface-level policy map also cannot be added to the hierarchical policy map. If you want these changes to occur, the hierarchical policy map must first be removed from the SVI.

For more information about hierarchical policy maps, see the “Policing on SVIs” section in the “Configuring QoS” chapter of the software configuration guide for this release.

Examples

This example shows how to create a policy map called *policy1*. When attached to the ingress port, it matches all the incoming traffic defined in *class1*, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mbps and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

This example shows how to configure multiple classes in a policy map called *polycymap2*:

```
Switch(config)# policy-map polycymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 100000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 100000 20000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp 0 (no policer)
Switch(config-pmap-c)# exit
```

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

```
Switch(config)# class-map cm-non-int
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-non-int-2
Switch(config-cmap)# match access-group 102
Switch(config-cmap)# exit
Switch(config)# class-map cm-test-int
Switch(config-cmap)# match input-interface gigabitethernet0/2 - gigabitethernet0/3
Switch(config-cmap)# exit
Switch(config)# policy-map pm-test-int
Switch(config-pmap)# class cm-test-int
Switch(config-pmap-c)# police 18000000 8000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map pm-test-pm-2
Switch(config-pmap)# class cm-non-int
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap)# class cm-non-int-2
Switch(config-pmap-c)# set dscp 15
Switch(config-pmap-c)# service-policy pm-test-int
Switch(config-pmap-c)# end
Switch(config-cmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input pm-test-pm-2
```

This example shows how to delete *polycymap2*:

```
Switch(config)# no policy-map polycymap2
```

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

Related Commands

| Command | Description |
|-----------------------------------|--|
| class | Defines a traffic classification match criteria (through the police , set , and trust policy-map class configuration command) 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 | Applies a policy map to a port. |
| show mls qos vlan | Displays the quality of service (QoS) policy maps attached to an SVI. |
| show policy-map | Displays 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 configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | 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)# port-channel load-balance dst-mac
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel 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 current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands . |

power inline

Use the **power inline** interface configuration command to configure the power management mode on the Power over Ethernet (PoE) ports. Use the **no** form of this command to return to the default settings.

```
power inline { auto [max max-wattage] | never | static [max max-wattage] }
```

```
no power inline { auto | never | static }
```

Syntax Description

| | |
|-------------------------------|--|
| auto | Enable powered-device detection. If enough power is available, automatically allocate power to the PoE port after device detection. |
| max <i>max-wattage</i> | (Optional) Limit the power allowed on the port. The range is 4000 to 15400 milliwatts. If no value is specified, the maximum is allowed. |
| never | Disable device detection, and disable power to the port. |
| static | Enable powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers the powered device. |

Defaults

The default is **auto** (enabled).

The maximum wattage is 15400 milliwatts.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|---|
| 12.1(19)EA1 | This command was introduced. |
| 12.2(25)SE | The static and max <i>max-wattage</i> options were added. |

Usage Guidelines

This command is supported only on PoE-capable ports. If you enter this command on a port that does not support PoE, this error message appears:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# power inline auto
                    ^
% Invalid input detected at '^' marker.
```

Use the **max** *max-wattage* option to disallow higher-power powered devices. With this configuration, when the powered device sends Cisco Discovery Protocol (CDP) messages requesting more power than the maximum wattage, the switch removes power from the port. If the powered-device IEEE class maximum is greater than the maximum wattage, the switch does not power the device. The power is reclaimed into the global power budget.



Note

The switch never powers any Class 0 or Class 3 device if the **power inline max** *max-wattage* command is configured for less than 15.4 W.

If the switch denies power to a powered device (the powered device requests more power through CDP messages or if the IEEE class maximum is greater than the maximum wattage), the PoE port is in a power-deny state. The switch generates a system message, and the Oper column in the **show power inline** user EXEC command output shows *power-deny*.

Use the **power inline static max** *max-wattage* command to give a port high priority. The switch allocates PoE to a port configured in static mode before allocating power to a port configured in auto mode. The switch reserves power for the static port when it is configured rather than upon device discovery. The switch reserves the power on a static port even when there is no connected device and whether or not the port is in a shutdown or in a no shutdown state. The switch allocates the configured maximum wattage to the port, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed power when it is connected to a static port. However, if the powered device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that the powered device needs more than the maximum wattage, the powered device is shut down.

If the switch cannot pre-allocate power when a port is in static mode (for example, because the entire power budget is already allocated to other auto or static ports), this message appears: `Command rejected: power inline static: pwr not available`. The port configuration remains unchanged.

When you configure a port by using the **power inline auto** or the **power inline static** interface configuration command, the port autonegotiates by using the configured speed and duplex settings. This is necessary to determine the power requirements of the connected device (whether or not it is a powered device). After the power requirements have been determined, the switch hardcodes the interface by using the configured speed and duplex settings without resetting the interface.

When you configure a port by using the **power inline never** command, the port reverts to the configured speed and duplex settings.

If a port has a Cisco powered device connected to it, you should not use the **power inline never** command to configure the port. A false link-up can occur on the port, placing it into an error-disabled state.



Caution

In releases earlier than Cisco IOS Release 12.2(20)SE1, power was sometimes still applied to a PoE port even after a powered device was removed. This could cause damage to a nonpowered device when it was later connected to that port. Make sure that your switch is running Cisco IOS Release 12.2(20)SE1 or later.

Examples

This example shows how to enable detection of a powered device and to automatically power a PoE port:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# power inline auto
```

This example shows how to configure a PoE port to allow a Class 1 or a Class 2 powered device:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# power inline auto max 7000
```

This example shows how to disable powered-device detection and to not power a PoE port:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# power inline never
```

You can verify your settings by entering the **show power inline** user EXEC command.

| Related Commands | Command | Description |
|------------------|---|--|
| | logging event power-inline-status | Enables the logging of PoE events. |
| | show controllers power inline | Displays the values in the registers of the specified PoE controller. |
| | show power inline | Displays the PoE status for the specified PoE port or for all PoE ports. |

priority-queue

Use the **priority-queue** interface configuration command to enable the egress expedite queue on a port. Use the **no** form of this command to return to the default setting.

priority-queue out

no priority-queue out

Syntax Description

| | |
|------------|-----------------------------------|
| out | Enable the egress expedite queue. |
|------------|-----------------------------------|

Defaults

The egress expedite queue is disabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-------------|------------------------------|
| 12.1(19)EA1 | This command was introduced. |

Usage Guidelines

When you configure the **priority-queue out** command, the shaped round robin (SRR) weight ratios are affected because there is one fewer queue participating in SRR. This means that *weight1* in the **srr-queue bandwidth shape** or the **srr-queue bandwidth shape** interface configuration command is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.

Follow these guidelines when the expedite queue is enabled or the egress queues are serviced based on their SRR weights:

- If the egress expedite queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
- If the egress expedite queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
- If the egress expedite queue is disabled and the SRR shaped weights are not configured, SRR services the queue in shared mode.

Examples

This example shows how to enable the egress expedite queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
```

This example shows how to disable the egress expedite queue after the SRR shaped and shared weights are configured. The shaped mode overrides the shared mode.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

You can verify your settings by entering the **show mls qos interface *interface-id* queueing** or the **show running-config** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|--|--|
| | show mls qos interface queueing | Displays the queueing strategy (SRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map. |
| | srr-queue bandwidth shape | Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port. |
| | srr-queue bandwidth share | Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port. |

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**}

This command is available only if the switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|----------------------------|---|
| association | Create an association between the primary VLAN and a secondary VLAN. |
| <i>secondary-vlan-list</i> | 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. |



Note

The switch must be in VTP transparent mode when you configure private VLANs.

Defaults

The default is to have no private VLANs configured.

Command Modes

VLAN configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

Before configuring private VLANs, you must disable VTP (VTP mode transparent). After you configure a private VLAN, you should not change the VTP mode to client or server.

VTP does not propagate private-VLAN configuration. You must manually configure private VLANs on all switches in the Layer 2 network to merge their Layer 2 databases and to prevent 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 in 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 *secondary_vlan_list* 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.

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

Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

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.

Do not configure a private VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN.

Do not configure a private VLAN as a voice VLAN.

Do not configure fallback bridging on switches with private VLANs.

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 mode 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, and VLANs 502 and 503 as community VLANs, and to associate them in a private VLAN:

```
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)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
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 mode private-vlan | Configures a private-VLAN port as a host port or promiscuous port. |

private-vlan mapping

Use the **private-vlan mapping** interface configuration command on a switch virtual interface (SVI) to create a mapping between a private-VLAN primary and secondary VLANs so that both VLANs share the same primary VLAN SVI. Use the **no** form of this command to remove private-VLAN mappings from the SVI.

private-vlan mapping {[add | remove] *secondary-vlan-list*}

no private-vlan mapping

This command is available only if the switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|----------------------------|--|
| <i>secondary-vlan-list</i> | Specify one or more secondary VLANs to be mapped to the primary VLAN SVI. |
| add | (Optional) Map the secondary VLAN to the primary VLAN SVI. |
| remove | (Optional) Remove the mapping between the secondary VLAN and the primary VLAN SVI. |



Note

The switch must be in VTP transparent mode when you configure private VLANs.

Defaults

The default is to have no private VLAN SVI mapping configured.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | This command was introduced. |

Usage Guidelines

The SVI of the primary VLAN is created at Layer 3.

Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

The *secondary_vlan_list* 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.

Traffic that is received on the secondary VLAN is routed by the SVI of the primary VLAN.

A secondary VLAN can be mapped to only one primary SVI. If you configure the primary VLAN as a secondary VLAN, all SVIs specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 private-VLAN association, the mapping configuration does not take effect.

Examples

This example shows how to map the interface of VLAN 20 to the SVI of VLAN 18:

```
Switch# configure terminal
Switch# interface vlan 18
Switch(config-if)# private-vlan mapping 20
Switch(config-vlan)# end
```

This example shows how to permit routing of secondary VLAN traffic from secondary VLANs 303 to 305 and 307 through VLAN 20 SVI:

```
Switch# configure terminal
Switch# interface vlan 20
Switch(config-if)# private-vlan mapping 303-305, 307
Switch(config-vlan)# end
```

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

Related Commands

| Command | Description |
|---|---|
| show interfaces private-vlan mapping | Display private-VLAN mapping information for the VLAN SVIs. |

queue-set

Use the **queue-set** interface configuration command to map a port to a queue-set. Use the **no** form of this command to return to the default setting.

queue-set *qset-id*

no queue-set *qset-id*

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>qset-id</i> | ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2. |
|---------------------------|----------------|---|

| | |
|-----------------|------------------------|
| Defaults | The queue-set ID is 1. |
|-----------------|------------------------|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.1(19)EA1 | This command was introduced. |

| | |
|-----------------|--|
| Examples | <p>This example shows how to map a port to queue-set 2:</p> <pre>Switch(config)# interface gigabitethernet0/1 Switch(config-if)# queue-set 2</pre> <p>You can verify your settings by entering the show mls qos interface <i>[interface-id]</i> buffers privileged EXEC command.</p> |
|-----------------|--|

| | | |
|-------------------------|--|--|
| Related Commands | Command | Description |
| | mls qos queue-set output buffers | Allocates buffers to a queue-set. |
| | mls qos queue-set output threshold | Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set. |
| | show mls qos interface buffers | Displays quality of service (QoS) information. |

rcommand

Use the **rcommand** user EXEC command to start a Telnet session and to execute commands on a cluster member switch from the cluster command switch. To end the session, enter the **exit** command.

```
rcommand {n | commander | mac-address hw-addr}
```

| Syntax Description | | |
|-----------------------------------|--|--|
| <i>n</i> | | Provide the number that identifies a cluster member. The range is 0 to 15. |
| commander | | Provide access to the cluster command switch from a cluster member switch. |
| mac-address <i>hw-addr</i> | | MAC address of the cluster member switch. |

| Command Modes | |
|---------------|--|
| User EXEC | |

| Command History | Release | Modification |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines This command is available only on the cluster command switch.

If the switch is the cluster command switch but the cluster member switch *n* does not exist, an error message appears. To obtain the switch number, enter the **show cluster members** privileged EXEC command on the cluster command switch.

You can use this command to access a cluster member switch from the cluster command-switch prompt or to access a cluster command switch from the member-switch prompt.

For Catalyst 2900 XL, 3500 XL, 2950, 2970, 3550, and 3750 switches, the Telnet session accesses the member-switch command-line interface (CLI) at the same privilege level as on the cluster command switch. For example, if you execute this command at user level on the cluster command switch, the cluster member switch is accessed at user level. If you use this command on the cluster command switch at privileged level, the command accesses the remote device at privileged level. If you use an intermediate enable-level lower than *privileged*, access to the cluster member switch is at user level.

For Catalyst 1900 and 2820 switches running standard edition software, the Telnet session accesses the menu console (the menu-driven interface) if the cluster command switch is at privilege level 15. If the cluster command switch is at privilege level 1, you are prompted for the password before being able to access the menu console. Cluster command switch privilege levels map to the cluster member switches running standard edition software as follows:

- If the cluster command switch privilege level is from 1 to 14, the cluster member switch is accessed at privilege level 1.
- If the cluster command switch privilege level is 15, the cluster member switch is accessed at privilege level 15.

The Catalyst 1900 and 2820 CLI is available only on switches running Enterprise Edition Software.

This command will not work if the vty lines of the cluster command switch have access-class configurations.

You are not prompted for a password because the cluster member switches inherited the password of the cluster command switch when they joined the cluster.

Examples

This example shows how to start a session with member 3. All subsequent commands are directed to member 3 until you enter the **exit** command or close the session.

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

Related Commands

| Command | Description |
|--------------------------------------|---|
| show cluster members | Displays information about the cluster members. |

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 |
|-----------------|-------------|------------------------------|
| | 12.1(19)EA1 | This command was introduced. |

Usage Guidelines You can configure RSPAN VLANs only in config-VLAN mode (entered by using the **vlan** global configuration command), not the VLAN configuration mode entered by using the **vlan database** privileged EXEC command.

If VTP is enabled, the RSPAN feature is propagated by VLAN Trunking Protocol (VTP) for VLAN-IDs that are lower than 1005. If the RSPAN VLAN ID is in the extended range, you must manually configure intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch).

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

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.

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 are made 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.

Related 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 (global configuration) | 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 [{ flash:/filename | ftp://user:password@host/filename |
nvrasm:/filename | rnp://user@host/filename | tftp://host/filename }] [validation none]
```

This command is available only if your switch is running the enhanced multilayer image (EMI).

Syntax Description

| | |
|--|--|
| 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. |
| nvrasm:/filename | (Optional) Specify that the database agent or the binding file is in the NVRAM. |
| rnp://user@host/filename | (Optional) Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server. |
| tftp://host/filename | (Optional) Specify that the database agent or the binding file is on a TFTP server. |
| 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. |

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|------------------------------|
| 12.2(20)SE | 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 in the file:

```
Switch# renew ip dhcp snooping database validation none
```

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

renew ip dhcp snooping database

| Related Commands | Command | Description |
|-------------------------|--|--|
| | ip dhcp 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 the DHCP snooping database agent. |

■ renew ip dhcp snooping database

■ renew ip dhcp snooping database