# interface

To select an interface to configure and to enter interface configuration mode, use the **interface** command.

**interface** *type number*

## Syntax Description

| | |
|---|---|
| *type* | Type of interface to be configured; see Table 2-6 for valid values. |
| *number* | Module and port number. |

## Defaults

No interface types are configured.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EW | Extended to include the 10-Gigabit Ethernet interface. |

## Usage Guidelines

Table 2-6 lists the valid values for *type*.

***Table 2-6 Valid type Values***

| Keyword | Definition |
|---|---|
| **ethernet** | Ethernet IEEE 802.3 interface. |
| **fastethernet** | 100-Mbps Ethernet interface. |
| **gigabitethernet** | Gigabit Ethernet IEEE 802.3z interface. |
| **tengigabitethernet** | 10-Gigabit Ethernet IEEE 802.3ae interface. |
| **ge-wan** | Gigabit Ethernet WAN IEEE 802.3z interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only. |
| **pos** | Packet OC-3 interface on the Packet over SONET Interface Processor; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only. |
| **atm** | ATM interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only. |
| **vlan** | VLAN interface; see the **interface vlan** command. |
| **port-channel** | Port channel interface; see the **interface port-channel** command. |
| **null** | Null interface; the valid value is **0**. |

## Examples

This example shows how to enter the interface configuration mode on the Fast Ethernet interface 2/4:

```
Switch(config)# interface fastethernet2/4
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| show interfaces | Displays interface information. |

# interface port-channel

To access or create a port-channel interface, use the **interface port-channel** command.

**interface port-channel** *channel-group*

## Syntax Description

| | |
|---|---|
| *channel-group* | Port-channel group number; valid values are from 1 to 64. |

## Defaults

This command has no default settings.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

You can also create the port channels by entering the **interface port-channel** command. This will create a Layer 3 port channel. To change the Layer 3 port channel into a Layer 2 port channel, use the **switchport** command before you assign the physical interfaces to the channel group. A port channel cannot be changed from Layer 3 to Layer 2 or vice versa when it contains member ports.

Only one port channel in a channel group is allowed.

**Caution** The Layer 3 port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces.

If you want to use CDP, you must configure it only on the physical Fast Ethernet interface and not on the port-channel interface.

## Examples

This example creates a port-channel interface with a channel-group number of 64:

```
Switch(config)# interface port-channel 64
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Assigns and configures an EtherChannel interface to an EtherChannel group. |
| **show etherchannel** | Displays EtherChannel information for a channel. |

# interface range

To run a command on multiple ports at the same time, use the **interface range** command.

**interface range** {**vlan** *vlan_id - vlan_id*} {*port-range* | **macro** *name*}

## Syntax Description

| | |
|---|---|
| **vlan** *vlan_id - vlan_id* | Specifies a VLAN range; valid values are from 1 to 4094. |
| *port-range* | Port range; for a list of valid values for *port-range*, see the "Usage Guidelines" section. |
| **macro** *name* | Specifies the name of a macro. |

## Defaults

This command has no default settings.

## Command Modes

Global configuration mode

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(12c)EW | Support for extended VLAN addresses added. |

## Usage Guidelines

You can use the **interface range** command on the existing VLAN SVIs only. To display the VLAN SVIs, enter the **show running config** command. The VLANs that are not displayed cannot be used in the **interface range** command.

The values that are entered with the **interface range** command are applied to all the existing VLAN SVIs.

Before you can use a macro, you must define a range using the **define interface-range** command.

All configuration changes that are made to a port range are saved to NVRAM, but the port ranges that are created with the **interface range** command do not get saved to NVRAM.

You can enter the port range in two ways:

- Specifying up to five port ranges
- Specifying a previously defined macro

You can either specify the ports or the name of a port-range macro. A port range must consist of the same port type, and the ports within a range cannot span the modules.

You can define up to five port ranges on a single command; separate each range with a comma.

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

```
interface range gigabitethernet 5/1 -20, gigabitethernet4/5 -20.
```

Use these formats when entering the *port-range*:

- *interface-type* {*mod*}/{*first-port*} - {*last-port*}
- *interface-type* {*mod*}/{*first-port*} - {*last-port*}

Valid values for *interface-type* are as follows:

- **FastEthernet**
- **GigabitEthernet**
- **Vlan** *vlan_id*

You cannot specify both a macro and an interface range in the same command. After creating a macro, you can enter additional ranges. If you have already entered an interface range, the CLI does not allow you to enter a macro.

You can specify a single interface in the *port-range* value. This makes the command similar to the **interface** *interface-number* command.

## Examples

This example shows how to use the **interface range** command to interface to FE 5/18 - 20:

```
Switch(config)# interface range fastethernet 5/18 - 20
Switch(config-if)#
```

This command shows how to run a port-range macro:

```
Switch(config)# interface range macro macro1
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **define interface-range** | Creates a macro of interfaces. |
| **show running config** (refer to Cisco IOS documentation) | Displays the running configuration for a switch. |

# interface vlan

To create or access a Layer 3 switch virtual interface (SVI), use the **interface vlan** command. To delete an SVI, use the **no** form of this command.

**interface vlan** *vlan_id*

**no interface vlan** *vlan_id*

## Syntax Description

| | |
|---|---|
| *vlan_id* | Number of the VLAN; valid values are from 1 to 4094. |

## Defaults

Fast EtherChannel is not specified.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(12c)EW | Support for extended addressing was added. |

## Usage Guidelines

The SVIs are created the first time that you enter the **interface vlan** *vlan_id* command for a particular VLAN. The *vlan_id* value corresponds to the VLAN tag that is associated with the data frames on an ISL or 802.1Q-encapsulated trunk or the VLAN ID that is configured for an access port. A message is displayed whenever a VLAN interface is newly created, so you can check that you entered the correct VLAN number.

If you delete an SVI by entering the **no interface vlan** *vlan_id* command, the associated interface is forced into an administrative down state and marked as deleted. The deleted interface will no longer be visible in a **show interface** command.

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.

## Examples

This example shows the output when you enter the **interface vlan** *vlan_id* command for a new VLAN number:

```
Switch(config)# interface vlan 23
% Creating new VLAN interface.
Switch(config)#
```

# ip arp inspection filter vlan

To permit ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and apply it to a VLAN, use the **ip arp inspection filter vlan** command. To disable this application, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| *arp-acl-name* | Access control list name. |
| *vlan-range* | VLAN number or range; valid values are from 1 to 4094. |
| *static* | (Optional) Specifies that the access control list should be applied statically. |

## Defaults

No defined ARP ACLs are applied to any VLAN.

## Command Modes

Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

When an ARP access control list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only the IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without validation.

This command specifies that the incoming ARP packets are compared against the ARP access control list, and the packets are permitted only if the access control list permits them.

If the access control lists deny the packets because of explicit denies, the packets are dropped. If the packets are denied because of an implicit deny, they are then matched against the list of DHCP bindings if the ACL is not applied statically.

## Examples

This example shows how to apply the ARP ACL “static-hosts” to VLAN 1 for DAI:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection filter static-hosts vlan 1
Switch(config)# end
Switch#
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

```
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active      static-hosts      No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Acl-Match        Deny
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| arp access-list | Defines an ARP access list or adds clauses at the end of a predefined list. |
| show ip arp inspection | Displays the status of dynamic ARP inspection for a specific range of VLANs. |

# ip arp inspection limit (interface)

To limit the rate of incoming ARP requests and responses on an interface and prevent DAI from consuming all of the system's resources in the event of a DoS attack, use the **ip arp inspection limit** command. To release the limit, use the **no** form of this command.

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

**no ip arp inspection limit**

## Syntax Description

| | |
|---|---|
| **rate** *pps* | Specifies an upper limit on the number of incoming packets processed per second. The rate can range from 1 to 10000. |
| **none** | Specifies no upper limit on the rate of the incoming ARP packets that can be processed. |
| **burst interval** *seconds* | (Optional) Specifies the consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets. The interval is configurable from 1 to 15 seconds. |

## Defaults

The rate is set to 15 packets per second on the 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 the trusted interfaces.

The burst interval is set to 1 second by default.

## Command Modes

Interface

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(20)EW | Added support for interface monitoring. |

## Usage Guidelines

The trunk ports should be configured with higher rates to reflect their aggregation. When the rate of the incoming packets exceeds the user-configured rate, the interface is placed into an error-disabled state. The error-disable timeout feature can be used to remove the port from the error-disabled state. The rate applies to both the trusted and nontrusted interfaces. Configure appropriate rates on trunks to handle the packets across multiple DAI-enabled VLANs or use the **none** keyword to make the rate unlimited.

The rate of the incoming ARP packets onthe channel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for the channel ports only after examining the rate of the incoming ARP packets on the channel members.

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

## Examples

This example shows how to limit the rate of the incoming ARP requests to 25 packets per second:

```
Switch# config terminal
Switch(config)# interface fa6/3
Switch(config-if)# ip arp inspection limit rate 25
Switch(config-if)# end
Switch# show ip arp inspection interfaces fastEthernet 6/3
Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Trusted                25
Switch#
```

This example shows how to limit the rate of the incoming ARP requests to 20 packets per second and to set the interface monitoring interval to 5 consecutive seconds:

```
Switch# config terminal
Switch(config)# interface fa6/1
Switch(config-if)# ip arp inspection limit rate 20 burst interval 5
Switch(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| show ip arp inspection | Displays the status of dynamic ARP inspection for a specific range of VLANs. |

# ip arp inspection log-buffer

To configure the parameters that are associated with the logging buffer, use the **ip arp inspection log-buffer** command. To disable the parameters, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| **entries** *number* | Number of entries from the logging buffer; the range is from 0 to 1024. |
| **logs** *number* | Number of entries to be logged in an interval; the range is from 0 to 1024. A 0 value indicates that entries should not be logged out of this buffer. |
| **interval** *seconds* | Logging rate; the range is from 0 to 86400 (1 day). A 0 value indicates an immediate log. |

## Defaults

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

The number of entries is set to 32.

The number of logging entries is limited to 5 per second.

The interval is set to 1.

## Command Modes

Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The first dropped packet of a given flow is logged immediately. The subsequent packets for the same flow are registered but are not logged immediately. Registering these packets is done in a log buffer that is shared by all the VLANs. Entries from this buffer are logged on a rate-controlled basis.

## Examples

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

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection log-buffer entries 45
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size : 45
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
Switch#
```

This example shows how to configure the logging rate to 10 logs per 3 seconds:

```
Switch(config)# ip arp inspection log-buffer logs 10 interval 3
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size : 45
Syslog rate : 10 entries per 3 seconds.
No entries in log buffer.
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| arp access-list | Defines an ARP access list or adds clauses at the end of a predefined list. |
| show ip arp inspection | Displays the status of dynamic ARP inspection for a specific range of VLANs. |

# ip arp inspection trust

To set a per-port configurable trust state that determines the set of interfaces where incoming ARP packets are inspected, use the **ip arp inspection trust** command. To make the interfaces untrusted, use the **no** form of this command.

**ip arp inspection trust**

**no ip arp inspection trust**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Interface

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to configure an interface to be trusted:

```
Switch# config terminal
Switch(config)# interface fastEthernet 6/3
Switch(config-if)# ip arp inspection trust
Switch(config-if)# end
```

To verify the configuration, use the show form of this command:

```
Switch# show ip arp inspection interfaces fastEthernet 6/3

 Interface        Trust State     Rate (pps)     Burst Interval
 ---------------  -----------     ----------     --------------
 Fa6/3            Trusted              None                  1
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| show ip arp inspection | Displays the status of dynamic ARP inspection for a specific range of VLANs. |

# ip arp inspection validate

To perform specific checks for ARP inspection, use the **ip arp inspection validate** command. To disable checks, use the **no** form of this command.

**ip arp inspection validate** [**src-mac**] [**dst-mac**] [**ip**]

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

## Syntax Description

| | |
|---|---|
| **src-mac** | (Optional) Checks the source MAC address in the Ethernet header against the sender's MAC address in the ARP body. This checking is done against both ARP requests and responses.<br>**Note** When **src-mac** is enabled, packets with different MAC addresses are classified as invalid and are dropped. |
| **dst-mac** | (Optional) Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This checking is done for ARP responses.<br>**Note** When **dst-mac** is enabled, the packets with different MAC addresses are classified as invalid and are dropped. |
| **ip** | (Optional) Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.<br>The sender IP addresses are checked in all ARP requests and responses and target IP addresses are checked only in ARP responses. |

## Defaults

Checks are disabled.

## Command Modes

Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

When enabling the checks, specify at least one of the keywords (**src-mac**, **dst-mac**, and **ip**) on the command line. Each command overrides the configuration of the previous command. If a command enables **src** and **dst mac** validations, and a second command enables IP validation only, the **src** and **dst mac** validations are disabled as a result of the second command.

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

## Examples

This example show how to enable the source MAC validation:

```
Switch(config)# ip arp inspection validate src-mac
Switch(config)# end
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| arp access-list | Defines an ARP access list or adds clauses at the end of a predefined list. |
| show ip arp inspection | Displays the status of dynamic ARP inspection for a specific range of VLANs. |

# ip arp inspection vlan

To enable dynamic ARP inspection (DAI) on a per-VLAN basis, use the **ip arp inspection vlan** command. To disable DAI, use the **no** form of this command.

**ip arp inspection vlan** *vlan-range*

**no ip arp inspection vlan** *vlan-range*

## Syntax Description

| | |
|---|---|
| *vlan-range* | VLAN number or range; valid values are from 1 to 4094. |

## Defaults

ARP inspection is disabled on all VLANs.

## Command Modes

Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if they have not been created or if they are private.

## Examples

This example shows how to enable DAI on VLAN 1:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
Switch# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active
Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
Switch#
```

This example shows how to disable DAI on VLAN 1:

```
Switch# configure terminal
Switch(config)# no ip arp inspection vlan 1
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| arp access-list | Defines an ARP access list or adds clauses at the end of a predefined list. |
| show ip arp inspection | Displays the status of dynamic ARP inspection for a specific range of VLANs. |

# ip arp inspection vlan logging

To control the type of packets that are logged, use the **ip arp inspection vlan logging** command. To disable this logging control, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| *vlan-range* | Number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094. |
| **acl-match** | Specifies the logging criteria for packets that are dropped or permitted based on ACL matches. |
| **matchlog** | Specifies that logging of packets matched against ACLs is controlled by the **matchlog** keyword in the permit and deny access control entries of the ACL.<br>**Note** By default, the **matchlog** keyword is not available on the ACEs. When the keyword is used, denied packets are not logged. Packets are logged only when they match against an ACE that has the **matchlog** keyword. |
| **none** | Specifies that ACL-matched packets are not logged. |
| **dhcp-bindings** | Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings. |
| **permit** | Specifies logging when permitted by DHCP bindings. |
| **all** | Specifies logging when permitted or denied by DHCP bindings. |
| **none** | Prevents all logging of packets permitted or denied by DHCP bindings. |

## Defaults

All denied or dropped packets are logged.

## Command Modes

Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The **acl-match** and **dhcp-bindings** keywords merge with each other. When you set an ACL match configuration, the DHCP bindings configuration is not disabled. You can use the **no** form of this command to reset some of the logging criteria to their defaults. If you do not specify either option, all the logging types are reset to log on when the ARP packets are denied. The two options that are available to you are as follows:

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

## Examples

This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log on matching against the ACLs with the **logging** keyword:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
Switch(config)# end
Switch# show ip arp inspection vlan 1

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

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Acl-Match        Deny
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| arp access-list | Defines an ARP access list or adds clauses at the end of a predefined list. |
| show ip arp inspection | Displays the status of dynamic ARP inspection for a specific range of VLANs. |

# ip cef load-sharing algorithm

To configure the load-sharing hash function so that the source TCP/UDP port, the destination TCP/UDP port, or both ports can be included in the hash in addition to the source and destination IP addresses, use the **ip cef load-sharing algorithm** command. To revert back to the default, which does not include the ports, use the **no** form of this command.

**ip cef load-sharing algorithm** {**include-ports** {**source** *source* | **destination** *dest*} | **original** | **tunnel** | **universal**}

**no ip cef load-sharing algorithm** {**include-ports** {**source** *source* | **destination** *dest*} | **original** | **tunnel** | **universal**}

## Syntax Description

| | |
|---|---|
| **include-ports** | Specifies the algorithm that includes the Layer 4 ports. |
| **source** *source* | Specifies the source port in the load-balancing hash functions. |
| **destination** *dest* | Specifies the destination port in the load-balancing hash. Uses the source and destination in hash functions. |
| **original** | Specifies the original algorithm; not recommended. |
| **tunnel** | Specifies the algorithm for use in tunnel-only environments. |
| **universal** | Specifies the default Cisco IOS load-sharing algorithm. |

## Defaults

Default load-sharing algorithm is disabled.

**Note** This option does not include the source or destination port in the load-balancing hash.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The original algorithm, tunnel algorithm, and universal algorithm are routed through the hardware. For software-routed packets, the algorithms are handled by the software. The **include-ports** option does not apply to the software-switched traffic.

## Examples

This example shows how to configure the IP CEF load-sharing algorithm that includes Layer 4 ports:

```
Switch(config)# ip cef load-sharing algorithm include-ports
Switch(config)#
```

This example shows how to configure the IP CEF load-sharing algorithm that includes Layer 4 tunneling ports:

```
Switch(config)# ip cef load-sharing algorithm include-ports tunnel
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| show ip cef vlan | Displays the IP CEF VLAN interface status and configuration information. |

# ip device tracking maximum

To enable IP port security binding tracking on a Layer 2 port, use the **ip device tracking maximum** command. To disable IP port security on untrusted Layer 2 interfaces, use the **no** form of this command.

**ip device tracking maximum** {*number*}

**no ip device tracking maximum** {*number*}

## Syntax Description

| | |
|---|---|
| *number* | Specifies the number of bindings created in the IP device tracking table for a port, valid values are from 0 to 2048. |

## Defaults

This command has no default settings.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(37)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to enable IP Port Security with IP-Mac filters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastethernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

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

## Related Commands

| Command | Description |
|---|---|
| **ip verify source** | Enables IP source guard on untrusted Layer 2 interfaces. |
| **show ip verify source** | Displays the IP source guard configuration and filters on a particular interface. |

# ip dhcp snooping

To enable DHCP snooping globally, use the **ip dhcp snooping** command. To disable DHCP snooping, use the **no** form of this command.

**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 mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You must enable DHCP snooping globally before you can use DHCP snooping on a VLAN.

## Examples

This example shows how to enable DHCP snooping:

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

This example shows how to disable DHCP snooping:

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

## Related Commands

| Command | Description |
|---|---|
| ip dhcp snooping information option | Enables DHCP option 82 data insertion. |
| ip dhcp snooping limit rate | Configures the number of the DHCP messages that an interface can receive per second. |
| ip dhcp snooping trust | Enables DHCP snooping on a trusted VLAN. |
| ip dhcp snooping vlan | Enables DHCP snooping on a VLAN or a group of VLANs. |
| show ip dhcp snooping | Displays the DHCP snooping configuration. |
| show ip dhcp snooping binding | Displays the DHCP snooping binding entries. |

# ip dhcp snooping binding

To set up and generate a DHCP binding configuration to restore bindings across reboots, use the **ip dhcp snooping binding** command. To disable the binding configuration, use the **no** form of this command.

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

**no ip dhcp snooping binding** *mac-address* **vlan** *vlan-# ip-address* **interface** *interface*

## Syntax Description

| | |
|---|---|
| *mac-address* | Specifies a MAC address. |
| **vlan** *vlan-#* | Specifies a valid VLAN number. |
| *ip-address* | Specifies an IP address. |
| **interface** *interface* | Specifies an interface type and number. |
| **expiry** *seconds* | Specifies the interval (in seconds) after which binding is no longer valid. |

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(25)EW | Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Whenever a binding is added or removed using this command, the binding database is marked as changed and a write is initiated.

## Examples

This example shows how to generate a DHCP binding configuration on interface gigabitethernet1/1 in VLAN 1 with an expiration time of 1000 seconds:

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping. |
| **ip dhcp snooping information option** | Enables DHCP option 82 data insertion. |
| **ip dhcp snooping trust** | Enables DHCP snooping on a trusted VLAN. |
| **ip dhcp snooping vlan** | Enables DHCP snooping on a VLAN or a group of VLANs. |

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding entries. |

# ip dhcp snooping database

To store the bindings that are generated by DHCP snooping, use the **ip dhcp snooping database** command. To either reset the timeout, reset the write-delay, or delete the agent specified by the URL, use the **no** form of this command.

**ip dhcp snooping database** {*url* | **timeout** *seconds* | **write-delay** *seconds*}

**no ip dhcp snooping database** {**timeout** | **write-delay**}

## Syntax Description

| | |
|---|---|
| *url* | Specifies the URL in one of the following forms:<br>• tftp://<host>/<filename><br>• ftp://<user>:<password>@<host>/<filename><br>• rcp://<user>@<host>/<filename><br>• nvram:/<filename><br>• bootflash:/<filename> |
| **timeout** *seconds* | Specifies when to abort the database transfer process after a change to the binding database.<br>The minimum value of the delay is 15 seconds. 0 is defined as an infinite duration. |
| **write-delay** *seconds* | Specifies the duration for which the transfer should be delayed after a change to the binding database. |

## Defaults

The timeout value is set to 300 seconds (5 minutes).

The write-delay value is set to 300 seconds.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You need to create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can write the set of bindings for the first time at the URL.

**Note** Because both NVRAM and bootflash have limited storage capacity, using TFTP or network-based files is recommended . If you use flash to store the database file, new updates (by the agent) result in the creation of new files (flash fills quickly). In addition, due to the nature of the filesystem used on the flash, a large number of files cause access to be considerably slowed. When a file is stored in a remote location accessible through TFTP, an RPR/SSO standby supervisor engine can take over the binding list when a switchover occurs.

## Examples

This example shows how to store a database file with the IP address 10.1.1.1 within a directory called directory. A file named file must be present on the TFTP server.

```
Switch# config terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
Switch# show ip dhcp snooping database
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : Yes
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        1   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0

Switch#
```

## Related Commands

| Command | Description |
|---|---|
| ip dhcp snooping | Globally enables DHCP snooping. |
| ip dhcp snooping binding | Sets up and generates a DHCP binding configuration to restore bindings across reboots. |
| ip dhcp snooping information option | Enables DHCP option 82 data insertion. |
| ip dhcp snooping trust | Enables DHCP snooping on a trusted VLAN. |
| ip dhcp snooping vlan | Enables DHCP snooping on a VLAN or a group of VLANs. |
| show ip dhcp snooping | Displays the DHCP snooping configuration. |
| show ip dhcp snooping binding | Displays the DHCP snooping binding entries. |

# ip dhcp snooping information option

To enable DHCP option 82 data insertion, use the **ip dhcp snooping information option** command. To disable DHCP option 82 data insertion, use the **no** form of this command.

**ip dhcp snooping information option format remote-id** {**hostname** | **string** {*word*}}

**no ip dhcp snooping information option format remote-id** {**hostname** | **string** {*word*}}

## Syntax Description

| | |
|---|---|
| **format** | Specifies the Option 82 information format. |
| **remote-id** | Specifies the remote ID for Option 82. |
| **hostname** | Specifies the user-configured hostname for the remote ID. |
| **string** *word* | Specifies the user defined string for the remote ID. The word string can be from 1 to 63 characters long with no spaces. |

## Defaults

DHCP option 82 data insertion is enabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(40)SG | Added **remote-id** keyword to support Option 82 enhancement. |

## Usage Guidelines

If the hostname is longer than 63 characters it is truncated to 63 characters in the Remote ID.

## Examples

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

```
Switch(config)# ip dhcp snooping information option
Switch(config)#
```

This example shows how to disable DHCP option 82 data insertion:

```
Switch(config)# no ip dhcp snooping information option
Switch(config)#
```

This example shows how to configure the hostname as the Remote ID:

```
Switch(config)# ip dhcp snooping information option format remote-id hostname
Switch(config)#
```

The following example shows how to enable DHCP Snooping on Vlan 500 through 555 and Opton 82 remote-id.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
```

```
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id string customer-500
Switch(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| ip dhcp snooping | Globally enables DHCP snooping. |
| ip dhcp snooping limit rate | Configures the number of the DHCP messages that an interface can receive per second. |
| ip dhcp snooping binding | Sets up and generates a DHCP binding configuration to restore bindings across reboots. |
| ip dhcp snooping information option | Enables DHCP option 82 data insertion. |
| ip dhcp snooping trust | Enables DHCP snooping on a trusted VLAN. |
| ip dhcp snooping vlan | Enables DHCP snooping on a VLAN or a group of VLANs. |
| ip dhcp snooping vlan number information option format-type | Enables circuit-id (a sub-option of DHCP snooping option-82) on a VLAN. |
| show ip dhcp snooping | Displays the DHCP snooping configuration. |
| show ip dhcp snooping binding | Displays the DHCP snooping binding entries. |

# ip dhcp snooping information option allow-untrusted

To allow DHCP packets with option 82 data inserted to be received from a snooping untrusted port, use the **ip dhcp snooping information option allow-untrusted** command. To disallow receipt of these DHCP packets, use the **no** form of this command.

**ip dhcp snooping information option allow-untrusted**

**no ip dhcp snooping information option allow-untrusted**

## Syntax Description

This command has no arguments or keywords.

## Defaults

DHCP packets with option 82 are not allowed on snooping untrusted ports.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EWA | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to allow DHCP packets with option 82 data inserted to be received from a snooping untrusted port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping information option allow-untrusted
Switch(config)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| ip dhcp snooping | Globally enables DHCP snooping. |
| ip dhcp snooping limit rate | Configures the number of the DHCP messages that an interface can receive per second. |
| ip dhcp snooping information option | Enables DHCP option 82 data insertion. |
| ip dhcp snooping trust | Enables DHCP snooping on a trusted VLAN. |
| ip dhcp snooping vlan | Enables DHCP snooping on a VLAN or a group of VLANs. |
| show ip dhcp snooping | Displays the DHCP snooping configuration. |
| show ip dhcp snooping binding | Displays the DHCP snooping binding entries. |

# ip dhcp snooping limit rate

To configure the number of the DHCP messages that an interface can receive per second, use the **ip dhcp snooping limit rate** command. To disable the DHCP snooping rate limiting, use the **no** form of this command.

**ip dhcp snooping limit rate** *rate*

**no ip dhcp snooping limit rate**

## Syntax Description

| | |
|---|---|
| *rate* | Number of DHCP messages a switch can receive per second. |

## Defaults

DHCP snooping rate limiting is disabled.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Typically, the rate limit applies to the untrusted interfaces. If you want to set up rate limiting for the trusted interfaces, note that the trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit of the interfaces to a higher value.

## Examples

This example shows how to enable the DHCP message rate limiting:

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

This example shows how to disable the DHCP message rate limiting:

```
Switch(config-if)# no ip dhcp snooping limit rate
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping. |
| **ip dhcp snooping information option** | Enables DHCP option 82 data insertion. |
| **ip dhcp snooping trust** | Enables DHCP snooping on a trusted VLAN. |
| **ip dhcp snooping vlan** | Enables DHCP snooping on a VLAN or a group of VLANs. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding entries. |

# ip dhcp snooping trust

To configure an interface as trusted for DHCP snooping purposes, use the **ip dhcp snooping trust** command. To configure an interface as untrusted, use the **no** form of this command.

**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 mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to enable DHCP snooping trust on an interface:

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

This example shows how to disable DHCP snooping trust on an interface:

```
Switch(config-if)# no ip dhcp snooping trust
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping. |
| **ip dhcp snooping information option** | Enables DHCP option 82 data insertion. |
| **ip dhcp snooping limit rate** | Configures the number of the DHCP messages that an interface can receive per second. |
| **ip dhcp snooping vlan** | Enables DHCP snooping on a VLAN or a group of VLANs. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding entries. |

# ip dhcp snooping vlan

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

**ip dhcp snooping** [**vlan** *number*]

**no ip dhcp snooping** [**vlan** *number*]

## Syntax Description

| | |
|---|---|
| **vlan** *number* | (Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094. |

## Defaults

DHCP snooping is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

DHCP snooping is enabled on a VLAN only if both global snooping and the VLAN snooping are enabled.

## Examples

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

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

This example shows how to disable DHCP snooping on a VLAN:

```
Switch(config)# no ip dhcp snooping vlan 10
Switch(config)#
```

This example shows how to enable DHCP snooping on a group of VLANs:

```
Switch(config)# ip dhcp snooping vlan 10 55
Switch(config)#
```

This example shows how to disable DHCP snooping on a group of VLANs:

```
Switch(config)# no ip dhcp snooping vlan 10 55
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| ip dhcp snooping | Globally enables DHCP snooping. |
| ip dhcp snooping information option | Enables DHCP option 82 data insertion. |
| ip dhcp snooping limit rate | Configures the number of the DHCP messages that an interface can receive per second. |
| ip dhcp snooping trust | Enables DHCP snooping on a trusted VLAN. |
| ip dhcp snooping vlan number information option format-type | Enables circuit-id (a sub-option of DHCP snooping option-82) on a VLAN. |
| show ip dhcp snooping | Displays the DHCP snooping configuration. |
| show ip dhcp snooping binding | Displays the DHCP snooping binding entries. |

# ip dhcp snooping vlan *number* information option format-type

To enable circuit-id (a sub-option of DHCP snooping option-82) on a VLAN, use the **ip dhcp snooping vlan** *number* **information option format-type** command. To disable circuit-id on a VLAN, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| **vlan** *number* | Single VLAN number or a range of VLANs; valid values are from 1 to 4094. |
| **information** | Specifies DHCP snooping information 82 data insertion. |
| **option** | Specifies DHCP snooping information option. |
| **format-type** | Specifies option-82 information format. |
| **circuit-id** | Specifies using the string as the circuit ID. |
| **string** *string* | Specifies a user-defined string for the circuit ID. |

## Defaults

VLAN-mod-port, if DHCP snooping option-82 is disabled.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The curcuit-id suboption of DHCP option-82 is supported only when DHCP snooping is globally enabled and on VLANs using DHCP option-82.

## Examples

The following example shows how to enable DHCP Snooping on Vlan 500 through 555 and Opton 82 circuit-id.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id string customer-500
Switch(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| ip dhcp snooping | Globally enables DHCP snooping. |
| ip dhcp snooping information option | Enables DHCP option 82 data insertion. |
| ip dhcp snooping limit rate | Configures the number of the DHCP messages that an interface can receive per second. |
| ip dhcp snooping trust | Enables DHCP snooping on a trusted VLAN. |
| ip dhcp snooping vlan | Enables DHCP snooping on a VLAN or a group of VLANs. |
| show ip dhcp snooping | Displays the DHCP snooping configuration. |
| show ip dhcp snooping binding | Displays the DHCP snooping binding entries. |

# ip igmp filter

To control whether all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an IGMP profile to the interface, use the **ip igmp filter** command. To remove a profile from the interface, use the **no** form of this command.

**ip igmp filter** *profile number*

**no ip igmp filter**

## Syntax Description

| | |
|---|---|
| *profile number* | IGMP profile number to be applied; valid values are from 1 to 429496795. |

## Defaults

Profiles are not applied.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(11b)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

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.

An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.

## Examples

This example shows how to apply IGMP profile 22 to an interface.

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp filter 22
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| ip igmp profile | Create an IGMP profile. |
| show ip igmp profile | Displays all configured IGMP profiles or a specified IGMP profile. |

# ip igmp max-groups

To set the maximum number of IGMP groups that a Layer 2 interface can join, use the **ip igmp max-groups** command. To set the maximum back to the default, use the **no** form of this command.

**ip igmp max-groups** *number*

**no ip igmp max-groups**

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of IGMP groups that an interface can join; valid values are from 0 to 4294967294. |

## Defaults

No maximum limit.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(11b)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You can use the **ip igmp max-groups** command only on Layer 2 physical interfaces; you cannot set the IGMP maximum groups for the routed ports, the switch virtual interfaces (SVIs), or the ports that belong to an EtherChannel group.

## Examples

This example shows how to limit the number of IGMP groups that an interface can join to 25:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)
```

# ip igmp profile

To create an IGMP profile, use the **ip igmp profile** command. To delete the IGMP profile, use the **no** form of this command.

**ip igmp profile** *profile number*

**no ip igmp profile** *profile number*

## Syntax Description

| | |
|---|---|
| *profile number* | IGMP profile number being configured; valid values are from 1 to 4294967295. |

## Defaults

No profile created.

## Command Modes

Global configuration mode

IGMP profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(11b)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

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 terminal
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
Switch(config-igmp-profile)#
```

## Related Commands

| Command | Description |
|---|---|
| ip igmp filter | Controls whether all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an IGMP profile to the interface. |
| show ip igmp profile | Displays all configured IGMP profiles or a specified IGMP profile. |

# ip igmp query-interval

To configure the frequency that the switch sends the IGMP host-query messages, use the **ip igmp query-interval** command. To return to the default frequency, use the **no** form of this command.

**ip igmp query-interval** *seconds*

**no ip igmp query-interval**

## Syntax Description

| | |
|---|---|
| *seconds* | Frequency, in seconds, at which the IGMP host-query messages are transmitted; valid values depend on the IGMP snooping mode. See the "Usage Guidelines" section for more information. |

## Defaults

The query interval is set to 60 seconds.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If you use the default IGMP snooping configuration, the valid query interval values are from 1 to 65535 seconds. If you have changed the default configuration to support CGMP as the IGMP snooping learning method, the valid query interval values are from 1 to 300 seconds.

The designated switch for a LAN is the only switch that sends the IGMP host-query messages. For IGMP version 1, the designated switch is elected according to the multicast routing protocol that runs on the LAN. For IGMP version 2, the designated querier is the lowest IP-addressed multicast switch on the subnet.

If no queries are heard for the timeout period (controlled by the **ip igmp query-timeout** command), the switch becomes the querier.

**Note** Changing the timeout period may severely impact multicast forwarding.

## Examples

This example shows how to change the frequency at which the designated switch sends the IGMP host-query messages:

```
Switch(config-if)# ip igmp query-interval 120
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp querier-timeout** (refer to Cisco IOS documentation) | Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying. |
| **ip pim query-interval** (refer to Cisco IOS documentation) | Configures the frequency of Protocol Independent Multicast (PIM) router query messages. |
| **show ip igmp groups** (refer to Cisco IOS documentation) | Displays the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show ip igmp groups** command in EXEC mode. |

# ip igmp snooping

To enable IGMP snooping, use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

**ip igmp snooping** [**tcn** {**flood query count** *count* | **query solicit**}]

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

## Syntax Description

| | |
|---|---|
| **tcn** | (Optional) Specifies the topology change configurations. |
| **flood** | (Optional) Specifies to flood the spanning-tree table to the network when a topology change occurs. |
| **query** | (Optional) Specifies the TCN query configurations. |
| **count** *count* | (Optional) Specifies how often the spanning-tree table is flooded; valid values are from 1 to 10. |
| **solicit** | (Optional) Specifies an IGMP general query. |

## Defaults

IGMP snooping is enabled.

## Command Modes

Global configuration mode

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(11)EW | Support for flooding the spanning-tree table was added. |

## Usage Guidelines

The **tcn flood** option applies only to Layer 2 switch ports and EtherChannels; it does not apply to routed ports, VLAN interfaces, or Layer 3 channels.

The **ip igmp snooping command** is disabled by default on multicast routers.

**Note** You can use the **tcn flood** option in interface configuration mode.

## Examples

This example shows how to enable IGMP snooping:

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

This example shows how to disable IGMP snooping:

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

This example shows how to enable the flooding of the spanning-tree table to the network after nine topology changes have occurred:

```
Switch(config)# ip igmp snooping tcn flood query count 9
Switch(config)#
```

This example shows how to disable the flooding of the spanning-tree table to the network:

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

This example shows how to enable an IGMP general query:

```
Switch(config)# ip igmp snooping tcn query solicit
Switch(config)#
```

This example shows how to disable an IGMP general query:

```
Switch(config)# no ip igmp snooping tcn query solicit
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| ip igmp snooping vlan immediate-leave | Enable IGMP immediate-leave processing. |
| ip igmp snooping vlan mrouter | Configures a Layer 2 interface as a multicast router interface for a VLAN. |
| ip igmp snooping vlan static | Configures a Layer 2 interface as a member of a group. |

# ip igmp snooping report-suppression

To enable report suppression, use the **ip igmp snooping report-suppression** command. To disable report suppression and forward the reports to the multicast devices, use the **no** form of this command.

**ip igmp snooping report-suppression**

**no igmp snooping report-suppression**

## Syntax Description

This command has no arguments or keywords.

## Defaults

IGMP snooping report-suppression is enabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If the **ip igmp snooping report-suppression** command is disabled, all the IGMP reports are forwarded to the multicast devices.

If the command is enabled, report suppression is done by IGMP snooping.

## Examples

This example shows how to enable report suppression:

```
Switch(config)# ip igmp snooping report-suppression
Switch(config)#
```

This example shows how to disable report suppression:

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

This example shows how to display the system status for report suppression:

```
Switch# show ip igmp snoop
vlan 1
----------
 IGMP snooping is globally enabled
 IGMP snooping TCN solicit query is globally disabled
 IGMP snooping global TCN flood query count is 2
 IGMP snooping is enabled on this Vlan
 IGMP snooping immediate-leave is disabled on this Vlan
 IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
 IGMP snooping is running in IGMP_ONLY mode on this Vlan
 IGMP snooping report suppression is enabled on this Vlan
Switch#
```

**Related Commands**

| Command | Description |
|---|---|
| ip igmp snooping vlan immediate-leave | Enable IGMP immediate-leave processing. |
| ip igmp snooping vlan mrouter | Configures a Layer 2 interface as a multicast router interface for a VLAN. |
| ip igmp snooping vlan static | Configures a Layer 2 interface as a member of a group. |

# ip igmp snooping vlan

To enable IGMP snooping for a VLAN, use the **ip igmp snooping vlan** command. To disable IGMP snooping, use the **no** form of this command.

**ip igmp snooping vlan** *vlan-id*

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

## Syntax Description

| | |
|---|---|
| *vlan-id* | Number of the VLAN; valid values are from 1 to 1001 and from 1006 to 4094. |

## Defaults

IGMP snooping is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(12c)EW | Support for extended addressing was added. |

## Usage Guidelines

This command is entered in VLAN interface configuration mode only.

The **ip igmp snooping vlan** command is disabled by default on multicast routers.

## Examples

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

```
Switch(config)# ip igmp snooping vlan 200
Switch(config)#
```

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

```
Switch(config)# no ip igmp snooping vlan 200
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| ip igmp snooping vlan immediate-leave | Enable IGMP immediate-leave processing. |
| ip igmp snooping vlan mrouter | Configures a Layer 2 interface as a multicast router interface for a VLAN. |
| ip igmp snooping vlan static | Configures a Layer 2 interface as a member of a group. |

# ip igmp snooping vlan explicit-tracking

To enable per-VLAN explicit host tracking, use the **ip igmp snooping vlan explicit-tracking** command. To disable explicit host tracking, use the **no** form of this command.

**ip igmp snooping vlan** *vlan-id* **explicit-tracking**

**no ip igmp snooping vlan** *vlan-id* **explicit-tracking**

## Syntax Description

| | |
|---|---|
| *vlan_id* | (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094. |

## Defaults

Explicit host tracking is enabled.

## Command Modes

Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(20)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to disable IGMP explicit host tracking on interface VLAN 200 and how to verify the configuration:

```
Switch(config)# no ip igmp snooping vlan 200 explicit-tracking
Switch(config)# end
Switch# show ip igmp snooping vlan 200 | include explicit tracking
Global IGMP Snooping configuration:
------------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2

Vlan 2:
--------
IGMP snooping                  : Enabled
IGMPv2 immediate leave         : Disabled
Explicit host tracking         : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode     : IGMP_ONLY
Explicit host tracking         : Disabled
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping vlan immediate-leave** | Enable IGMP immediate-leave processing. |
| **ip igmp snooping vlan mrouter** | Configures a Layer 2 interface as a multicast router interface for a VLAN. |

| Command | Description |
|---|---|
| ip igmp snooping vlan static | Configures a Layer 2 interface as a member of a group. |
| show ip igmp snooping membership | Displays host membership information. |

# ip igmp snooping vlan immediate-leave

To enable IGMP immediate-leave processing, use the **ip igmp snooping vlan immediate-leave** command. To disable immediate-leave processing, use the **no** form of this command.

**ip igmp snooping vlan** *vlan_num* **immediate-leave**

**no ip igmp snooping vlan** *vlan_num* **immediate-leave**

## Syntax Description

| | |
|---|---|
| *vlan_num* | Number of the VLAN; valid values are from 1 to 4094. |
| **immediate-leave** | Enables immediate leave processing. |

## Defaults

Immediate leave processing is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(12c)EW | Support for extended addressing was added. |

## Usage Guidelines

You enter this command in global configuration mode only.

Use the immediate-leave feature only when there is a single receiver for the MAC group for a specific VLAN.

The immediate-leave feature is supported only with IGMP version 2 hosts.

## Examples

This example shows how to enable IGMP immediate-leave processing on VLAN 4:

```
Switch(config)# ip igmp snooping vlan 4 immediate-leave
Switch(config)#
```

This example shows how to disable IGMP immediate-leave processing on VLAN 4:

```
Switch(config)# no ip igmp snooping vlan 4 immediate-leave
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| ip igmp snooping | Enable IGMP snooping. |
| ip igmp snooping vlan mrouter | Configures a Layer 2 interface as a multicast router interface for a VLAN. |
| ip igmp snooping vlan static | Configures a Layer 2 interface as a member of a group. |

| Command | Description |
|---|---|
| show ip igmp interface | Displays the information about the IGMP-interface status and configuration. |
| show mac-address-table multicast | Displays information about the multicast MAC address table. |

# ip igmp snooping vlan mrouter

To statically configure an Layer 2 interface as a multicast router interface for a VLAN, use the **ip igmp snooping vlan mrouter** command. To remove the configuration, use the **no** form of this command.

**ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** {{**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *slot/port*} | {**port-channel** *number*}} | {**learn** {**cgmp** | **pim-dvmrp**}}

**noip igmp snooping vlan** *vlan-id* **mrouter** {**interface** {{**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *slot/port*} | {**port-channel** *number*}} | {**learn** {**cgmp** | **pim-dvmrp**}}

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | Specifies the VLAN ID number to use in the command; valid values are from 1 to 4094. |
| **interface** | Specifies the next-hop interface to a multicast switch. |
| **fastethernet** *slot/port* | Specifies the Fast Ethernet interface; number of the slot and port. |
| **gigabitethernet** *slot/port* | Specifies the Gigabit Ethernet interface; number of the slot and port. |
| **tengigabitethernet** *slot/port* | Specifies the 10-Gigabit Ethernet interface; number of the slot and port. |
| **port-channel** *number* | Port-channel number; valid values are from 1 to 64. |
| **learn** | Specifies the multicast switch learning method. |
| **cgmp** | Specifies the multicast switch snooping CGMP packets. |
| **pim-dvmrp** | Specifies the multicast switch snooping PIM-DVMRP packets. |

## Defaults

Multicast switch snooping PIM-DVMRP packets are specified.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(12c)EW | Support for extended addressing was added. |
| 12.2(25)EW | Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You enter this command in VLAN interface configuration mode only.

The interface to the switch must be in the VLAN where you are entering the command. It must be both administratively up and line protocol up.

The CGMP learning method can decrease control traffic.

The learning method that you configure is saved in NVRAM.

The static connections to multicast interfaces are supported only on switch interfaces.

## Examples

This example shows how to specify the next-hop interface to a multicast switch:

```
Switch(config-if)# ip igmp snooping 400 mrouter interface fastethernet 5/6
Switch(config-if)#
```

This example shows how to specify the multicast switch learning method:

```
Switch(config-if)# ip igmp snooping 400 mrouter learn cgmp
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping** | Enable IGMP snooping. |
| **ip igmp snooping vlan immediate-leave** | Enable IGMP immediate-leave processing. |
| **ip igmp snooping vlan static** | Configures a Layer 2 interface as a member of a group. |
| **show ip igmp snooping** | Displays information on dynamically learned and manually configured VLAN switch interfaces. |
| **show ip igmp snooping mrouter** | Displays information on the dynamically learned and manually configured multicast switch interfaces. |

# ip igmp snooping vlan static

To configure a Layer 2 interface as a member of a group, use the **ip igmp snooping vlan static** command. To remove the configuration, use the **no** form of this command.

**ip igmp snooping vlan** *vlan_num* **static** *mac-address* {**interface** {**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *slot/port*} | {**port-channel** *number*}}

**no ip igmp snooping vlan** *vlan_num* **static** *mac-address* {**interface** {**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *mod/interface-number*} | {**port-channel** *number*}}

## Syntax Description

| | |
|---|---|
| **vlan** *vlan_num* | Number of the VLAN. |
| **static** *mac-address* | Group MAC address. |
| **interface** | Specifies the next-hop interface to multicast switch. |
| **fastethernet** *slot/port* | Specifies the Fast Ethernet interface; number of the slot and port. |
| **gigabitethernet** *slot/port* | Specifies the Gigabit Ethernet interface; number of the slot and port. |
| **tengigabitethernet** *slot/port* | Specifies the 10-Gigabit Ethernet interface; number of the slot and port. |
| **port-channel** *number* | Port-channel number; valid values are from 1 through 64. |

## Defaults

This command has no default settings.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(25)EW | Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to configure a host statically on an interface:

```
Switch(config)# ip igmp snooping vlan 4 static 0100.5e02.0203 interface fastethernet 5/11
Configuring port FastEthernet5/11 on group 0100.5e02.0203 vlan 4
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| ip igmp snooping | Enable IGMP snooping. |
| ip igmp snooping vlan immediate-leave | Enable IGMP immediate-leave processing. |

| Command | Description |
|---|---|
| ip igmp snooping vlan mrouter | Configures a Layer 2 interface as a multicast router interface for a VLAN. |
| show mac-address-table multicast | Displays information about the multicast MAC address table. |

# ip local-proxy-arp

To enable the local proxy ARP feature, use the **ip local-proxy-arp** command. To disable the local proxy ARP feature, use the **no** form of this command.

**ip local-proxy-arp**

**no ip local-proxy-arp**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Local proxy ARP is disabled.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the switch on which they are connected.

ICMP redirect is disabled on interfaces where the local proxy ARP feature is enabled.

## Examples

This example shows how to enable the local proxy ARP feature:

```
Switch(config-if)# ip local-proxy-arp
Switch(config-if)#
```

# ip mfib fastdrop

To enable MFIB fast drop, use the **ip mfib fastdrop** command. To disable MFIB fast drop, use the **no** form of this command.

**ip mfib fastdrop**

**no ip mfib fastdrop**

## Syntax Description

This command has no arguments or keywords.

## Defaults

MFIB fast drop is enabled.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to enable MFIB fast drops:

```
Switch# ip mfib fastdrop
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| clear ip mfib fastdrop | Clears all the MFIB fast-drop entries. |
| show ip mfib fastdrop | Displays all currently active fast-drop entries and shows whether fast drop is enabled. |

# ip route-cache flow

To enable NetFlow statistics for IP routing, use the **ip route-cache flow** command. To disable NetFlow statistics, use the **no** form of this command.

**ip route-cache flow** [**infer-fields**]

**no ip route-cache flow** [**infer-fields**]

## Syntax Description

| | |
|---|---|
| **infer-fields** | (Optional) Includes the NetFlow fields as inferred by the software: Input identifier, Output identifier, and Routing information. |

## Defaults

NetFlow statistics is disabled.

Inferred information is excluded.

## Command Modes

Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(13)EW | Support for this command was introduced on the Catalyst 4500 series switches. |
| 12.1(19)EW | Command enhanced to support infer fields. |

## Usage Guidelines

To use these commands, you need to install the Supervisor Engine IV and the NetFlow Service Card.

The NetFlow statistics feature captures a set of traffic statistics. These traffic statistics include the source IP address, destination IP address, Layer 4 port information, protocol, input and output identifiers, and other routing information that can be used for network analysis, planning, accounting, billing and identifying DoS attacks.

NetFlow switching is supported on IP and IP-encapsulated traffic over all interface types.

If you enter the **ip route-cache flow infer-fields** command after the **ip route-cache flow** command, you will purge the existing cache, and vice versa. This action is done to avoid having flows with and without inferred fields in the cache simultaneously.

For additional information on NetFlow switching, refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

**Note** NetFlow consumes additional memory and CPU resources compared to other switching modes. You need to know the resources required on your switch before enabling NetFlow.

## Examples

This example shows how to enable NetFlow switching on the switch:

```
Switch# config terminal
Switch(config)# ip route-cache flow
Switch(config)# exit
Switch#
```

**Note** This command does not work on individual interfaces.

# ip source binding

To add or delete a static IP source binding entry, use the **ip source binding** command. To delete the corresponding IP source binding entry, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| *ip-address* | Binding IP address. |
| *mac-address* | Binding MAC address. |
| **vlan** *vlan-id* | VLAN number. |
| **interface** *interface-name* | Binding interface. |

## Defaults

This command has no default settings.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The **ip source binding** command is used to add a static IP source binding entry only.

The **no** form of this command deletes the corresponding IP source binding entry. For the deletion to succeed, all required parameters must match.

Each static IP binding entry is keyed by a MAC address and VLAN number. If the CLI contains an existing MAC and VLAN, the existing binding entry will be updated with the new parameters; a separate binding entry will not be created.

## Examples

This example shows how to configure the static IP source binding:

```
Switch# config terminal
Switch(config)# ip source binding 11.0.0.1 0000.000A.000B vlan 10 interface
fastethernet6/10
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| show ip source binding | Displays IP source bindings that are configured on the system. |

# ip sticky-arp

To enable sticky ARP, use the **ip sticky-arp** command. Use the **no** form of this command to disable sticky ARP.

**ip sticky-arp**

**no ip sticky-arp**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is supported on PVLANs only.

ARP entries that are learned on Layer3 PVLAN interfaces are sticky ARP entries. (You should display and verify ARP entries on the PVLAN interface using the **show arp** command).

For security reasons, sticky ARP entries on the PVLAN interface do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created.

Because the ARP entries on the PVLAN interface do not age out, you must manually remove ARP entries on the PVLAN interface if a MAC address changes.

Unlike static entries, sticky-ARP entries are not stored and restored when you enter the **reboot** and **restart** commands.

## Examples

This example shows how to enable sticky ARP:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) ip sticky-arp
Switch(config)# end
Switch#
```

This example shows how to disable sticky ARP:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) no ip sticky-arp
Switch(config)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **arp** (refer to Cisco IOS documentation) | Enables Address Resolution Protocol (ARP) entries for static routing over the Switched Multimegabit Data Service (SMDS) network. |
| **show arp** (refer to Cisco IOS documentation) | Displays ARP information. |

# ip verify header vlan all

To enable IP header validation for Layer 2-switched IPv4 packets, use the **ip verify header vlan all** command. To disable the IP header validation, use the **no** form of this command.

**ip verify header vlan all**

**no ip verify header vlan all**

## Syntax Description

This command has no default settings.

## Defaults

The IP header is validated for bridged and routed IPv4 packets.

## Command Modes

Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(20)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command does not apply to Layer 3-switched (routed) packets.

The Catalyst 4500 series switch checks the validity of the following fields in the IPv4 header for all switched IPv4 packets:

- The version must be 4.
- The header length must be greater than or equal to 20 bytes.
- The total length must be greater than or equal to four times the header length and greater than the Layer 2 packet size minus the Layer 2 encapsulation size.

If an IPv4 packet fails the IP header validation, the packet is dropped. If you disable the header validation, the packets with the invalid IP headers are bridged but are not routed even if routing was intended. The IPv4 access lists also are not applied to the IP headers.

## Examples

This example shows how to disable the IP header validation for the Layer 2-switched IPv4 packets:

```
Switch# config terminal
Switch(config)# no ip verify header vlan all
Switch(config)# end
Switch#
```

# ip verify source

To enable IP source guard on untrusted Layer 2 interfaces, use the **ip verify source** command. To disable IP source guard on untrusted Layer 2 interfaces, use the **no** form of this command.

**ip verify source** {**vlan dhcp-snooping** | **tracking**} [**port-security**]

**no ip verify source** {**vlan dhcp-snooping** | **tracking**} [**port-security**]

## Syntax Description

| | |
|---|---|
| **vlan dhcp-snooping** | Enables IP source guard on untrusted Layer 2 DHCP snooping interfaces. |
| **tracking** | Enables IP port security to learn static IP address learning on a port. |
| **port-security** | (Optional) Filters both source IP and MAC addresses using the port security feature. |

## Defaults

IP source guard is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(37)SG | Added support for IP port security and tracking. |

## Examples

This example shows how to enable IP source guard on VLANs 10 through 20 on a per-port basis:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# interface fastethernet6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip verify source interface f6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa6/1      ip-mac       active       10.0.0.1                            10
Fa6/1      ip-mac       active       deny-all                            11-20
Switch#
```

This example shows how to enable IP Port Security with IP-Mac filters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

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

## Related Commands

| Command | Description |
|---|---|
| **ip device tracking maximum** | Enables IP port security binding tracking on a Layer 2 port. |
| **ip dhcp snooping** | Globally enables DHCP snooping. |
| **ip dhcp snooping limit rate** | Configures the number of the DHCP messages that an interface can receive per second. |
| **ip dhcp snooping information option** | Enables DHCP option 82 data insertion. |
| **ip dhcp snooping trust** | Enables DHCP snooping on a trusted VLAN. |
| **ip source binding** | Adds or delete a static IP source binding entry. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding entries. |
| **show ip verify source** | Displays the IP source guard configuration and filters on a particular interface. |
| **show ip source binding** | Displays IP source bindings that are configured on the system. |

# ip verify unicast source reachable-via

To enable and configure unicast RPF checks on a Supervisor Engine 6-E and Catalyst 4900M chassis IPv4 interface, use the **ip verify unicast source reachable-via** command. To disable unicast RPF, use the **no** form of this command.

**ip verify unicast source reachable-via rx allow-default**

**no ip verify unicast source reachable-via**

## Syntax Description

| | |
|---|---|
| **rx** | Verifies that the source address is reachable on the interface where the packet was received. |
| **allow-default** | Verifies that the default route matches the source address. |

## Defaults

Disabled

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | Support for this command was introduced on the Catalyst 4500 with a Supervisor Engine 6-E or a Catalyst 4900M chassis. |

## Usage Guidelines

In basic RX mode, unicast RPF ensures a source address must be reachable on the arrived interface. For example, the source must be reachable without load balancing.

**Note** Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

Do not use unicast RPF on internal network interfaces. Internal interfaces might have routing asymmetry, which means that there are multiple routes to the source of a packet. Apply unicast RPF only where there is natural or configured symmetry.

## Examples

This example shows how to enable unicast RPF exist-only checking mode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip verify unicast source reachable-via rx allow-default
Switch(config-if)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **ip cef** (refer to Cisco IOS documentation) | Enables Cisco Express Forwarding (CEF) on the switch. |
| **show running-config** | Displays the current running configuration for a switch. |

# ipv6 mld snooping

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN, use the **ipv6 mld snooping** command without keywords. To disable MLD snooping on a switch or the VLAN, use the **no** form of this command.

**ipv6 mld snooping** [**vlan** *vlan-id*]

**no ipv6 mld snooping** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Enables or disables IPv6 MLD snooping on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. |

## Defaults

MLD snooping is globally disabled on the switch.

MLD snooping is enabled on all VLANs. However, MLD snooping must be globally enabled before VLAN snooping can take place.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500. |

## Usage Guidelines

When MLD snooping is globally disabled, it is disabled on all the existing VLAN interfaces. When you globally enable MLD snooping, it is enabled on all VLAN interfaces that are in the default state (enabled). VLAN configuration overrides global configuration on interfaces on which MLD snooping has been disabled.

If MLD snooping is globally disabled, you cannot enable it on a VLAN. If MLD snooping is globally enabled, you can disable it on individual VLANs.

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

## Examples

This example shows how to globally enable MLD snooping:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping
Switch(config)#end
Switch#
```

This example shows how to disable MLD snooping on a VLAN:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ipv6 mld snooping vlan 11
Switch(config)#end
```

```
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping** user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show ipv6 mld snooping** | Displays IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN. |

# ipv6 mld snooping last-listener-query-count

To configure IP version 6 (IPv6) Multicast Listener Discovery Mulitcast Address Specific Queries (MASQs) that will be sent before aging out a client, use the **ipv6 mld snooping last-listener-query-count** command. To reset the query count to the default settings, use the **no** form of this command.

**ipv6 mld snooping** [**vlan** *vlan-id*] **last-listener-query-count** *integer_value*

**no ipv6 mld snooping** [**vlan** *vlan-id*] **last-listener-query-count**

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Configure last-listener query count on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| *integer_value* | The range is 1 to 7. |

## Command Default

The default global count is 2.

The default VLAN count is 0 (the global count is used).

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500. |

## Usage Guidelines

In MLD snooping, the IPv6 multicast switch periodically sends out queries to hosts belonging to the multicast group. If a host wants to leave a multicast group, it can silently leave or it can respond to the query with a Multicast Listener Done message (equivalent to an IGMP Leave message). When Immediate Leave is not configured (it should not be configured if multiple clients for a group exist on the same port), the configured last-listener query count determines the number of MASQs that are sent before an MLD client is aged out.

When the last-listener query count is set for a VLAN, this count overrides the value configured globally. When the VLAN count is not configured (set to the default of 0), the global count is used.

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

## Examples

This example shows how to globally set the last-listener query count:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping last-listener-query-count 1
Switch(config)#end
Switch#
```

This example shows how to set the last-listener query count for VLAN 10:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 10 last-listener-query-count 3
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **ipv6 mld snooping last-listener-query-interval** | Configures IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN. |
| **show ipv6 mld snooping** | Displays IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN. |
| **show ipv6 mld snooping querier** | Displays IP version 6 (IPv6) MLD snooping querier-related information most recently received by the switch or the VLAN. |

# ipv6 mld snooping last-listener-query-interval

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN, use the **ipv6 mld snooping last-listener-query-interval** command. To reset the query time to the default settings, use the **no** form of this command.

**ipv6 mld snooping** [**vlan** *vlan-id*] **last-listener-query-interval** *integer_value*

**no ipv6 mld snooping** [**vlan** *vlan-id*] **last-listener-query-interval**

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Configure last-listener query interval on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| *integer_value* | Set the time period (in thousandths of a second) that a multicast switch must wait after issuing a MASQ before deleting a port from the multicast group. The range is 100 to 32,768. The default is 1000 (1 second), |

## Command Default

The default global query interval (maximum response time) is 1000 (1 second).

The default VLAN query interval (maximum response time) is 0 (the global count is used).

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500. |

## Usage Guidelines

The last-listener-query-interval time is the maximum time that a multicast switch waits after issuing a Mulitcast Address Specific Query (MASQ) before deleting a port from the multicast group.

In MLD snooping, when the IPv6 multicast switch receives an MLD leave message, it sends out queries to hosts belonging to the multicast group. If there are no responses from a port to a MASQ for a length of time, the switch deletes the port from the membership database of the multicast address. The last listener query interval is the maximum time that the switch waits before deleting a nonresponsive port from the multicast group.

When a VLAN query interval is set, the global query interval is overridden. When the VLAN interval is set at 0, the global value is used.

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

## Examples

This example shows how to globally set the last-listener query interval to 2 seconds:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping last-listener-query-interval 2000
Switch(config)#end
```

```
Switch#
```

This example shows how to set the last-listener query interval for VLAN 1 to 5.5 seconds:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 last-listener-query-interval 5500
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **ipv6 mld snooping last-listener-query-count** | Configures IP version 6 (IPv6) Multicast Listener Discovery Mulitcast Address Specific Queries (MASQs) that will be sent before aging out a client. |
| **show ipv6 mld snooping querier** | Displays IP version 6 (IPv6) MLD snooping querier-related information most recently received by the switch or the VLAN. |

# ipv6 mld snooping listener-message-suppression

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping listener message suppression, use the **ipv6 mld snooping listener-message-suppression** command. To disable MLD snooping listener message suppression, use the **no** form of this command.

**ipv6 mld snooping listener-message-suppression**

**no ipv6 mld snooping listener-message-suppression**

## Command Default

The default is for MLD snooping listener message suppression to be disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500. |

## Usage Guidelines

MLD snooping listener message suppression is equivalent to IGMP snooping report suppression. When it is enabled, received MLDv1 reports to a group are forwarded to IPv6 multicast switchs only once in every report-forward time. This prevents the forwarding of duplicate reports.

## Examples

This example shows how to enable MLD snooping listener message suppression:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping listener-message-suppression
Switch(config)#end
Switch#
```

This example shows how to disable MLD snooping listener message suppression:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ipv6 mld snooping listener-message-suppression
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| ipv6 mld snooping | Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN. |
| show ipv6 mld snooping | Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN. |

# ipv6 mld snooping robustness-variable

To configure the number of IP version 6 (IPv6) Multicast Listener Discovery (MLD) queries that the switch sends before deleting a listener that does not respond, or to enter a VLAN ID to configure the number of queries per VLAN, use the **ipv6 mld snooping robustness-variable** command. To reset the variable to the default settings, use the **no** form of this command.

**ipv6 mld snooping** [**vlan** *vlan-id*] **robustness-variable** *integer_value*

**no ipv6 mld snooping** [**vlan** *vlan-id*] **robustness-variable**

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Configure the robustness variable on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| *integer_value* | The range is 1 to 3. |

## Command Default

The default global robustness variable (number of queries before deleting a listener) is 2.

The default VLAN robustness variable (number of queries before aging out a multicast address) is 0, which means that the system uses the global robustness variable for aging out the listener.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500. |

## Usage Guidelines

Robustness is measured by the number of MLDv1 queries sent with no response before a port is removed from a multicast group. A port is deleted when there are no MLDv1 reports received for the configured number of MLDv1 queries. The global value determines the number of queries that the switch waits before deleting a listener that does not respond, and it applies to all VLANs that do not have a VLAN value set.

The robustness value configured for a VLAN overrides the global value. If the VLAN robustness value is 0 (the default), the global value is used.

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

## Examples

This example shows how to configure the global robustness variable so that the switch sends out three queries before it deletes a listener port that does not respond:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping robustness-variable 3
Switch(config)#end
Switch#
```

This example shows how to configure the robustness variable for VLAN 1. This value overrides the global configuration for the VLAN:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 robustness-variable 1
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **ipv6 mld snooping last-listener-query-count** | Configures IP version 6 (IPv6) Multicast Listener Discovery Mulitcast Address Specific Queries (MASQs) that will be sent before aging out a client. |
| **show ipv6 mld snooping** | Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN. |

# ipv6 mld snooping tcn

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) Topology Change Notifications (TCNs), use the **ipv6 mld snooping tcn** commands. To reset the default settings, use the **no** form of the commands.

**ipv6 mld snooping tcn** {**flood query count** *integer_value* | **query solicit**}

**no ipv6 mld snooping tcn** {**flood query count** *integer_value* | **query solicit**}

## Syntax Description

| | |
|---|---|
| **flood query count** *integer_value* | Set the flood query count, which is the number of queries that are sent before forwarding multicast data to only those ports requesting it. The range is 1 to 10. |
| **query solicit** | Enable soliciting of TCN queries. |

## Command Default

TCN query soliciting is disabled.

When enabled, the default flood query count is 2.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SG | This command was introduced on the Catalyst 4500. |

## Examples

This example shows how to enable TCN query soliciting:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping tcn query solicit.
Switch(config)#end
Switch#
```

This example shows how to set the flood query count to 5:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping tcn flood query count 5.
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| show ipv6 mld snooping | Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN. |

# ipv6 mld snooping vlan

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping parameters on the VLAN interface, use the **ipv6 mld snooping vlan** command. To reset the parameters to the default settings, use the **no** form of this command.

**ipv6 mld snooping vlan** *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

**no ipv6 mld snooping vlan** *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | Specify a VLAN number. The range is 1 to 1001 and 1006 to 4094. |
| **immediate-leave** | (Optional) Enable MLD Immediate-Leave processing on a VLAN interface. Use the **no** form of the command to disable the Immediate Leave feature on the interface. |
| **mrouter interface** | (Optional) Configure a multicast switch port. The **no** form of the command removes the configuration. |
| **static** *ipv6-multicast-address* | (Optional) Configure a multicast group with the specified IPv6 multicast address. |
| **interface** *interface-id* | Add a Layer 2 port to the group. The mrouter or static interface can be a physical port or a **port-channel** interface ranging from 1 to 48. |

## Command Default

MLD snooping Immediate-Leave processing is disabled.

By default, there are no static IPv6 multicast groups.

By default, there are no multicast switch ports.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500. |

## Usage Guidelines

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

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

The configuration and the static ports and groups are saved in NVRAM.

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

## Examples

This example shows how to enable MLD Immediate-Leave processing on VLAN 1:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 immediate-leave
Switch(config)#end
Switch#
```

This example shows how to disable MLD Immediate-Leave processing on VLAN 1:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ipv6 mld snooping vlan 1 immediate-leave
Switch(config)#end
Switch#
```

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

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/0/2
Switch(config)#end
Switch#
```

This example shows how to configure a static multicast group:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/0/2
Switch(config)#end
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping vlan** *vlan-id* user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **ipv6 mld snooping** | Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN. |
| **show ipv6 mld snooping** | Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN. |

# issu abortversion

To cancel the ISSU upgrade or the downgrade process in progress and to restore the Catalyst 4500 series switch to its state before the start of the process, use the **issue abortversion** command.

**issu abortversion** *active-slot* [*active-image-new*]

## Syntax Description

| | |
|---|---|
| *active-slot* | Specifies the slot number for the current standby supervisor engine. |
| *active-image-new* | (Optional) Name of the new image present in the current standby supervisor engine. |

## Defaults

There are no default settings.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SGA | This command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You can use the **issu abortversion** command at any time to stop the ISSU process. To complete the process enter the **issu commitversion** command. Before any action is taken, a check ensures that both supervisor engines are either in the run version (RV) or load version (LV) state.

When the **issu abortversion** command is entered before the **issu runversion** command, the standby supervisor engine is reset and reloaded with the old image. When the **issu abortversion** command is entered after the **issu runversion** command, a change takes place and the new standby supervisor engine is reset and reloaded with the old image.

## Examples

This example shows how you can reset and reload the standby supervisor engine:

```
Switch# issu abortversion 2
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| issu acceptversion | Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process. |
| issu commitversion | Loads the new Cisco IOS software image into the new standby supervisor engine. |
| issu loadversion | Starts the ISSU process. |

| Command | Description |
|---|---|
| issu runversion | Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified. |
| show issu state | Displays the ISSU state and current booted image name during the ISSU process. |

# issu acceptversion

To halt the rollback timer and to ensure that the new Cisco IOS software image is not automatically stopped during the ISSU process, use the **issu acceptversion** command.

**issu acceptversion** *active-slot* [*active-image-new*]

## Syntax Description

| | |
|---|---|
| *active-slot* | Specifies the slot number for the currently active supervisor engine. |
| *active-image-new* | (Optional) Name of the new image on the current lyactive supervisor engine. |

## Defaults

Rollback timer resets automatically 45 minutes after you issue the **issu runversion** command.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SGA | This command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

After you are satisfied with the new image and have confirmed the new supervisor engine is reachable by both the console and the network, enter the **issu acceptversion** command to halt the rollback timer. If the **issu acceptversion** command is not entered within 45 minutes from the time the **issu runversion** command is entered, the entire ISSU process is automatically rolled back to the previous version of the software. The rollback timer starts immediately after you issue the **issu runversion** command.

If the rollback timer expires before the standby supervisor engine goes to a hot standby state, the timer is automatically extended by up to 15 minutes. If the standby state goes to a hot-standby state within this extension time or the 15 minute extension expires, the switch aborts the ISSU process. A warning message that requires your intervention is displayed every 1 minute of the timer extension.

If the rollback timer is set to a long period of time, such as the default of 45 minutes, and the standby supervisor engine goes into the hot standby state in 7 minutes, you have 38 minutes (45 minus 7) to roll back if necessary.

Use the **issu set rollback-timer** to configure the rollback timer.

## Examples

This example shows how to halt the rollback timer and allow the ISSU process to continue:

```
Switch# issu acceptversion 2
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| issu abortversion | Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process. |
| issu commitversion | Loads the new Cisco IOS software image into the new standby supervisor engine. |
| issu loadversion | Starts the ISSU process. |
| issu runversion | Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified. |
| issu set rollback-timer | Configures the In Service Software Upgrade (ISSU) rollback timer value. |
| show issu state | Displays the ISSU state and current booted image name during the ISSU process. |

# issu commitversion

To load the new Cisco IOS software image into the new standby supervisor engine, use the **issu commitversion** command.

**issu commitversion** *standby-slot standby-image-new*

## Syntax Description

| | |
|---|---|
| *standby-slot* | Specifies the slot number for the currently active supervisor engine. |
| *active-image-new* | (Optional) Name of the new image on the currently active supervisor engine. |

## Defaults

Enabled by default.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SGA | This command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The **issu commitversion** command verifies that the standby supervisor engine has the new Cisco IOS software image in its file system and that both supervisor engines are in the run version (RV) state. If these conditions are met, the following actions take place:

- The standby supervisor engine is reset and booted with the new version of Cisco IOS software.
- The standby supervisor engine moves into the Stateful Switchover (SSO) mode and is fully stateful for all clients and applications with which the standby supervisor engine is compatible.
- The supervisor engines are moved into final state, which is the same as initial state.

Entering the **issu commitversion** command completes the In Service Software Upgrade (ISSU) process. This process cannot be stopped or reverted to its original state without starting a new ISSU process.

Entering the **issu commitversion** command without entering the **issu acceptversion** command is equivalent to entering both the **issu acceptversion** and the **issu commitversion** commands. Use the **issu commitversion** command if you do not intend to run in the current state for an extended period of time and are satisfied with the new software version.

## Examples

This example shows how you can configure the standby supervisor engine to be reset and reloaded with the new Cisco IOS software version:

```
Switch# issu commitversion 1
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| issu acceptversion | Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process. |
| issu commitversion | Loads the new Cisco IOS software image into the new standby supervisor engine. |
| issu loadversion | Starts the ISSU process. |
| issu runversion | Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified. |
| show issu state | Displays the ISSU state and current booted image name during the ISSU process. |

# issu loadversion

To start the ISSU process, use the **issu loadversion** command.

**issu loadversion** *active-slot active-image-new standby-slot standby-image-new* [**force**]

## Syntax Description

| | |
|---|---|
| *active-slot* | Specifies the slot number for the currently active supervisor engine. |
| *active-image-new* | Specifies the name of the new image on the currently active supervisor engine. |
| *standby-slot* | Specifies the standby slot on the networking device. |
| *standby-image-new* | Specifies the name of the new image on the standby supervisor engine. |
| **force** | (Optional) Overrides the automatic rollback when the new Cisco IOS software version is detected to be incompatible. |

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SGA | This command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The **issu loadversion** command causes the standby supervisor engine to be reset and booted with the new Cisco IOS software image specified by the command. If both the old image and the new image are ISSU capable, ISSU compatible, and have no configuration mismatches, the standby supervisor engine moves into Stateful Switchover (SSO) mode, and both supervisor engines move into the load version (LV) state.

It will take several seconds after the **issu loadversion** command is entered for Cisco IOS software to load onto the standby supervisor engine and the standby supervisor engine to transition to SSO mode.

## Examples

This example shows how to initiate the ISSU process:

```
Switch# issu loadversion 1 bootflash:new-image 2 slavebootflash:new-image
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **issu abortversion** | Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process. |
| **issu acceptversion** | Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process. |

| Command | Description |
|---|---|
| issu commitversion | Loads the new Cisco IOS software image into the new standby supervisor engine. |
| issu runversion | Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified. |
| show issu state | Displays the ISSU state and current booted image name during the ISSU process. |

# issu runversion

To force a change from the active supervisor engine to the standby supervisor engine and to cause the newly active supervisor engine to run the new image specified in the **issu loadversion** command, use the **issu runversion** command.

**issu runversion** *standby-slot* [*standby-image-new*]

## Syntax Description

| | |
|---|---|
| *standby-slot* | Specifies the standby slot on the networking device. |
| *standby-image-new* | Specifies the name of the new image on the standby supervisor engine. |

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SGA | This command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The **issu runversion** command changes the currently active-supervisor engine to standby-supervisor engine and the real standby-supervisor engine is booted with the old image version following and resets the switch. As soon as the standby-supervisor engine moves into the standby state, the rollback timer is started.

## Examples

This example shows how to force a change of the active-supervisor engine to standby-supervisor engine:

```
Switch# issu runversion 2
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **issu abortversion** | Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process. |
| **issu acceptversion** | Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process. |
| **issu commitversion** | Loads the new Cisco IOS software image into the new standby supervisor engine. |
| **issu loadversion** | Starts the ISSU process. |
| **show issu state** | Displays the ISSU state and current booted image name during the ISSU process. |

# issu set rollback-timer

To configure the In Service Software Upgrade (ISSU) rollback timer value, use the **issu set rollback-timer** command.

**issu set rollback-timer** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Specfies the rollback timer value, in seconds. The valid timer value range is from 0 to 7200 seconds (2 hours). A value of 0 seconds disables the rollback timer. |

## Defaults

Rollback timer value is 2700 seconds.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SGA | This command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Use the **issue set rollback-timer** command to configure the rollback timer value. You can only enable this command when the supervisor engines are in the init state.

## Examples

This example shows how you can set the rollback timer value to 3600 seconds, or 1 hour:

```
Switch# configure terminal
Switch(config)# issu set rollback-timer 3600
Switch(config)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **issu acceptversion** | Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process. |
| **issu set rollback-timer** | Configures the In Service Software Upgrade (ISSU) rollback timer value. |

# l2protocol-tunnel

To enable protocol tunneling on an interface, use the **l2protocol-tunnel** command. You can enable tunneling for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable tunneling on the interface, use the **no** form of this command.

**l2protocol-tunnel** [**cdp** | **stp** | **vtp**]

**no l2protocol-tunnel** [**cdp** | **stp** | **vtp**]

## Syntax Description

| | |
|---|---|
| **cdp** | (Optional) Enables tunneling of CDP. |
| **stp** | (Optional) Enables tunneling of STP. |
| **vtp** | (Optional) Enables tunneling of VTP. |

## Defaults

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

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

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

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.

## Examples

This example shows how to enable protocol tunneling for the CDP packets:

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| l2protocol-tunnel cos | Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets. |

| Command | Description |
|---|---|
| l2protocol-tunnel drop-threshold | Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets. |
| l2protocol-tunnel shutdown-threshold | Configures the protocol tunneling encapsulation rate. |

# l2protocol-tunnel cos

To configure the class of service (CoS) value for all tunneled Layer 2 protocol packets, use the **l2protocol-tunnel cos** command. To return to the default value of zero, use the **no** form of this command.

**l2protocol-tunnel cos** *value*

**no l2protocol-tunnel cos**

## Syntax Description

| | |
|---|---|
| *value* | Specifies the CoS priority value for tunneled Layer 2 protocol packets. The range is 0 to 7, with 7 being the highest priority. |

## Defaults

The default is to use the CoS value that is 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 mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | This command was first introduced on the Catalyst 4500 series switch. |

## 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
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| l2protocol-tunnel | Enables protocol tunneling on an interface. |
| l2protocol-tunnel drop-threshold | Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets. |
| l2protocol-tunnel shutdown-threshold | Configures the protocol tunneling encapsulation rate. |

# l2protocol-tunnel drop-threshold

To set a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets, use the **l2protocol-tunnel drop-threshold** command. You can set the drop threshold for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable the drop threshold on the interface, use the **no** form of this command.

**l2protocol-tunnel** drop**-threshold** [**cdp | stp | vtp**] *value*

**no l2protocol-tunnel** drop**-threshold** [**cdp | stp | vtp**] *value*

## Syntax Description

| | |
|---|---|
| **cdp** | (Optional) Specifies a drop threshold for CDP. |
| **stp** | (Optional) Specifies a drop threshold for STP. |
| **vtp** | (Optional) Specifies a drop threshold for VTP. |
| *value* | Specifies a threshold in packets per second to be received for encapsulation before the interface shuts down, or specifies the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold. |

## Defaults

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

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The **l2protocol-tunnel drop-threshold** command controls 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 the Layer 2 protocol packets until the rate at which they are received is below the drop threshold.

## Examples

This example shows how to configure the drop threshold rate:

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

## Related Commands

| Command | Description |
|---|---|
| l2protocol-tunnel | Enables protocol tunneling on an interface. |
| l2protocol-tunnel cos | Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets. |
| l2protocol-tunnel shutdown-threshold | Configures the protocol tunneling encapsulation rate. |

# l2protocol-tunnel shutdown-threshold

To configure the protocol tunneling encapsulation rate, use the **l2protocol-tunnel shutdown-threshold** command. You can set the encapsulation rate for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable the encapsulation rate on the interface, use the **no** form of this command.

**l2protocol-tunnel shutdown-threshold** [**cdp | stp | vtp**] *value*

**no l2protocol-tunnel shutdown-threshold** [**cdp | stp | vtp**] *value*

## Syntax Description

| | |
|---|---|
| **cdp** | (Optional) Specifies a shutdown threshold for CDP. |
| **stp** | (Optional) Specifies a shutdown threshold for STP. |
| **vtp** | (Optional) Specifies a shutdown threshold for VTP. |
| *value* | Specifies a threshold in packets per second to be received for encapsulation before the interface shuts down. The range is 1 to 4096. The default is no threshold. |

## Defaults

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

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The **l2-protocol-tunnel shutdown-threshold** command controls 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** 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 feature generation is not enabled for **l2ptguard**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** commands.

## Examples

This example shows how to configure the maximum rate:

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

## Related Commands

| Command | Description |
|---|---|
| l2protocol-tunnel | Enables protocol tunneling on an interface. |
| l2protocol-tunnel cos | Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets. |
| l2protocol-tunnel drop-threshold | Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets. |

# lacp port-priority

To set the LACP priority for the physical interfaces, use the **lacp port-priority** command.

**lacp port-priority** *priority*

## Syntax Description

| | |
|---|---|
| *priority* | Priority for the physical interfaces; valid values are from 1 to 65535. |

## Defaults

Priority is set to 32768.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(13)EW | This command was introduced on the Catalyst 4500 series switches. |

## Usage Guidelines

This command is not supported on the systems that are configured with a Supervisor Engine I.

You must assign each port in the switch a port priority that can be specified automatically or by entering the **lacp port-priority** command. The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Although this command is a global configuration command, the *priority* value is supported only on port channels with LACP-enabled physical interfaces.This command is supported on LACP-enabled interfaces.

When setting the priority, the higher numbers indicate lower priorities.

## Examples

This example shows how to set the priority for the interface:

```
Switch(config-if)# lacp port-priority 23748
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Assigns and configure an EtherChannel interface to an EtherChannel group. |
| **channel-protocol** | Enables LACP or PAgP on an interface. |
| **lacp system-priority** | Sets the priority of the system for LACP. |
| **show lacp** | Displays LACP information. |

# lacp system-priority

To set the priority of the system for LACP, use the **lacp system-priority** command.

**lacp system-priority** *priority*

## Syntax Description

| | |
|---|---|
| *priority* | Priority of the system; valid values are from 1 to 65535. |

## Defaults

Priority is set to 32768.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(13)EW | This command was introduced on the Catalyst 4500 series switches. |

## Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine I.

You must assign each switch that is running LACP a system priority that can be specified automatically or by entering the **lacp system-priority** command. The system priority is used with the switch MAC address to form the system ID and is also used during negotiation with other systems.

Although this command is a global configuration command, the *priority* value is supported on port channels with LACP-enabled physical interfaces.

When setting the priority, tthe higher numbers indicate lower priorities.

You can also enter the **lacp system-priority** command in interface configuration mode. After you enter the command, the system defaults to global configuration mode.

## Examples

This example shows how to set the system priority:

```
Switch(config)# lacp system-priority 23748
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Assigns and configure an EtherChannel interface to an EtherChannel group. |
| **channel-protocol** | Enables LACP or PAgP on an interface. |
| **lacp system-priority** | Sets the priority of the system for LACP. |
| **show lacp** | Displays LACP information. |

# lldp run

To enable processing of received LLDP control packets and enable transmission of LLDP packets with default or configured TLVs..

**lldp run**

## Syntax Description

This command has no arguments or keywords.

## Defaults

LLDP is disabled.

## Command Modes

global interface level

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SG | Support was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Configuring this command enables LLDP protocol on the switch. Unconfiguring it disables processing or transmit of LLDP protocol packets from the switch.

## Examples

This example shows how to enable LLDP on the switch:

```
Switch(config)# lldp run
```

# logging event link-status global (global configuration)

To change the default switch-wide global link-status event messaging settings, use the **logging event link-status global** command. Use the **no** form of this command to disable the link-status event messaging.

**logging event link-status global**

**no logging event link-status global**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The global link-status messaging is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If link-status logging event is not configured at the interface level, this global link-status setting takes effect for each interface.

## Examples

This example shows how to globally enable link status message on each interface:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# logging event link-status global
Switch(config)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| logging event link-status (interface configuration) | Enables the link-status event messaging on an interface. |

# logging event link-status (interface configuration)

To enable the link-status event messaging on an interface, use the **logging event link-status** command. Use the **no** form of this command to disable link-status event messaging. Use the **logging event link-status use-global** command to apply the global link-status setting.

**logging event link-status**

**no logging event link-status**

**logging event link-status use-global**

## Defaults

Global link-status messaging is enabled.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

To enable system logging of interface state-change events on a specific interface, enter the **logging event link-status** command in interface configuration mode.

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event link-status global** command in global configuration mode. All interfaces without the state change event configuration use the global setting.

## Examples

This example shows how to enable logging event state-change events on interface gi11/1:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event link-status
Switch(config-if)# end
Switch#
```

This example shows how to turn off logging event link status regardless of the global setting:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# no logging event link-status
Switch(config-if)# end
Switch#
```

This example shows how to enable the global event link-status setting on interface gi11/1:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event link-status use-global
Switch(config-if)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| logging event link-status global (global configuration) | Changes the default switch-wide global link-status event messaging settings. |

# logging event trunk-status global (global configuration)

To enable the trunk-status event messaging globally, use the **logging event trunk-status global** command. Use the **no** form of this command to disable trunk-status event messaging.

**logging event trunk-status global**

**no logging event trunk-status global**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Global trunk-status messaging is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If trunk-status logging event is not configured at the interface level, the global trunk-status setting takes effect for each interface.

## Examples

This example shows how to globally enable link status messaging on each interface:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# logging event trunk-status global
Switch(config)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| logging event trunk-status global (global configuration) | Enables the trunk-status event messaging on an interface. |

# logging event trunk-status (interface configuration)

To enable the trunk-status event messaging on an interface, use the **logging event trunk-status** command. Use the **no** form of this command to disable the trunk-status event messaging. Use the **logging event trunk-status use-global** command to apply the global trunk-status setting.

**logging event trunk-status**

**no logging event trunk-status**

**logging event trunk-status use-global**

## Defaults

Global trunk-status messaging is enabled.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

To enable system logging of interface state-change events on a specific interface, enter the **logging event trunk-status** command in interface configuration mode.

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event trunk-status use-global** command in global configuration mode. All interfaces without the state change event configuration use the global setting.

## Examples

This example shows how to enable logging event state-change events on interface gi11/1:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event trunk-status
Switch(config-if)# end
Switch#
```

This example shows how to turn off logging event trunk status regardless of the global setting:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# no logging event trunk-status
Switch(config-if)# end
Switch#
```

This example shows how to enable the global event trunk-status setting on interface gi11/1:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event trunk-status use-global
Switch(config-if)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| logging event trunk-status global (global configuration) | Enables the trunk-status event messaging on an interface. |

# mac access-list extended

To define the extended MAC access lists, use the **mac access-list extended** command. To remove the MAC access lists, use the **no** form of this command.

**mac access-list extended** *name*

**no mac access-list extended** *name*

## Syntax Description

| | |
|---|---|
| *name* | ACL to which the entry belongs. |

## Defaults

MAC access lists are not defined.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long and can include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

When you enter the **mac access-list extended** *name* command, you use the [**no**] {**permit** | **deny**} {{*src-mac mask* | **any**} [*dest-mac mask*]} [**protocol-family** {**appletalk** | **arp-non-ipv4** | **decnet** | **ipx** | **ipv6** | **rarp-ipv4** | **rarp-non-ipv4** | **vines** | **xns**}] subset to create or delete entries in a MAC layer access list.

Table 2-7 describes the syntax of the **mac access-list extended** subcommands.

*Table 2-7 mac access-list extended Subcommands*

| Subcommand | Description |
|---|---|
| **deny** | Prevents access if the conditions are matched. |
| **no** | (Optional) Deletes a statement from an access list. |
| **permit** | Allows access if the conditions are matched. |
| *src-mac mask* | Source MAC address in the form:<br>*source-mac-address source-mac-address-mask*. |
| **any** | Specifies any protocol type. |

*Table 2-7 mac access-list extended Subcommands (continued)*

| Subcommand | Description |
|---|---|
| *dest-mac mask* | (Optional) Destination MAC address in the form: *dest-mac-address dest-mac-address-mask*. |
| *protocol-family* | (Optional) Name of the protocol family. Table 2-8 lists which packets are mapped to a particular protocol family. |

Table 2-8 describes mapping an Ethernet packet to a protocol family.

*Table 2-8 Mapping an Ethernet Packet to a Protocol Family*

| Protocol Family | Ethertype in Packet Header |
|---|---|
| Appletalk | 0x809B, 0x80F3 |
| Arp-Non-Ipv4 | 0x0806 and protocol header of Arp is a non-Ip protocol family |
| Decnet | 0x6000-0x6009, 0x8038-0x8042 |
| Ipx | 0x8137-0x8138 |
| Ipv6 | 0x86DD |
| Rarp-Ipv4 | 0x8035 and protocol header of Rarp is Ipv4 |
| Rarp-Non-Ipv4 | 0x8035 and protocol header of Rarp is a non-Ipv4 protocol family |
| Vines | 0x0BAD, 0x0BAE, 0x0BAF |
| Xns | 0x0600, 0x0807 |

When you enter the *src-mac mask* or *dest-mac mask* value, follow these guidelines:

- Enter the MAC addresses as three 4-byte values in dotted hexadecimal format such as 0030.9629.9f84.
- Enter the MAC address masks as three 4-byte values in dotted hexadecimal format. Use 1 bit as a wildcard. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- For the optional *protocol* parameter, you can enter either the EtherType or the keyword.
- Entries without a *protocol* parameter match any protocol.
- The access list entries are scanned in the order that you enter them. The first matching entry is used. To improve performance, place the most commonly used entries near the beginning of the access list.
- An implicit **deny any any** entry exists at the end of an access list unless you include an explicit **permit any any** entry at the end of the list.
- All new entries to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

## Examples

This example shows how to create a MAC layer access list named mac_layer that denies traffic from 0000.4700.0001, which is going to 0000.4700.0009, and permits all other traffic:

```
Switch(config)# mac access-list extended mac_layer
Switch(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 protocol-family appletalk
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch#
```

**Related Commands**

| Command | Description |
|---|---|
| **show vlan access-map** | Displays VLAN access map information. |

# mac-address-table aging-time

To configure the aging time for the entries in the Layer 2 table, use the **mac-address-table aging-time** command. To reset the *seconds* value to the default setting, use the **no** form of this command.

**mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]

**no mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]

## Syntax Description

| | |
|---|---|
| *seconds* | Aging time in seconds; valid values are 0 and from 10 to 1000000 seconds. |
| **vlan** *vlan_id* | (Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094. |

## Defaults

Aging time is set to 300 seconds.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(12c)EW | Support for extended addressing was added. |

## Usage Guidelines

If you do not enter a VLAN, the change is applied to all routed-port VLANs.

Enter 0 seconds to disable aging.

## Examples

This example shows how to configure the aging time to 400 seconds:

```
Switch(config)# mac-address-table aging-time 400
Switch(config)#
```

This example shows how to disable aging:

```
Switch(config)# mac-address-table aging-time 0
Switch(config)
```

## Related Commands

| Command | Description |
|---|---|
| show mac-address-table aging-time | Displays MAC address table aging information. |

# mac-address-table dynamic group protocols

To enable the learning of MAC addresses in both the "ip" and "other" protocol buckets, even though the incoming packet may belong to only one of the protocol buckets, use the **mac-address-table dynamic group protocols** command. To disable grouped learning, use the **no** form of this command.

**mac-address-table dynamic group protocols** {**ip** | **other**} {**ip** | **other**}

[**no**] **mac-address-table dynamic group protocols** {**ip** | **other**} {**ip** | **other**}

## Syntax Description

| | |
|---|---|
| **ip** | Specifies the "ip" protocol bucket. |
| **other** | Specifies the "other" protocol bucket. |

## Defaults

The group learning feature is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The entries within the "ip" and "other" protocol buckets are created according to the protocol of the incoming traffic.

When you use the **mac-address-table dynamic group protocols** command, an incoming MAC address that might belong to either the "ip" or the "other" protocol bucket, is learned on both protocol buckets. Therefore, any traffic destined to this MAC address and belonging to any of the protocol buckets is unicasted to that MAC address, rather than flooded. This reduces the unicast Layer 2 flooding that might be caused if the incoming traffic from a host belongs to a different protocol bucket than the traffic that is destined to the sending host.

## Examples

This example shows that the MAC addresses are initially assigned to either the "ip" or the "other" protocol bucket:

```
Switch# show mac-address-table dynamic
Unicast Entries
 vlan   mac address     type        protocols               port
-------+---------------+--------+---------------------+--------------------
   1    0000.0000.5000   dynamic other                 GigabitEthernet1/1
   1    0001.0234.6616   dynamic ip                    GigabitEthernet3/1
   1    0003.3178.ec0a   dynamic assigned              GigabitEthernet3/1
   1    0003.4700.24c3   dynamic ip                    GigabitEthernet3/1
   1    0003.4716.f475   dynamic ip                    GigabitEthernet3/1
   1    0003.4748.75c5   dynamic ip                    GigabitEthernet3/1
   1    0003.47f0.d6a3   dynamic ip                    GigabitEthernet3/1
   1    0003.47f6.a91a   dynamic ip                    GigabitEthernet3/1
```

```
   1    0003.ba06.4538   dynamic ip                    GigabitEthernet3/1
   1    0003.fd63.3eb4   dynamic ip                    GigabitEthernet3/1
   1    0004.2326.18a1   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5d.de53   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5e.6ecc   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5e.f60e   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5f.06f7   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5f.072f   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5f.08f6   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5f.090b   dynamic ip                    GigabitEthernet3/1
   1    0004.5a88.b075   dynamic ip                    GigabitEthernet3/1
   1    0004.c1bd.1b40   dynamic ip                    GigabitEthernet3/1
   1    0004.c1d8.b3c0   dynamic ip                    GigabitEthernet3/1
   1    0004.c1d8.bd00   dynamic ip                    GigabitEthernet3/1
   1    0007.e997.74dd   dynamic ip                    GigabitEthernet3/1
   1    0007.e997.7e8f   dynamic ip                    GigabitEthernet3/1
   1    0007.e9ad.5e24   dynamic ip                    GigabitEthernet3/1
   1    000b.5f0a.f1d8   dynamic ip                    GigabitEthernet3/1
   1    000b.fdf3.c498   dynamic ip                    GigabitEthernet3/1
   1    0010.7be8.3794   dynamic assigned              GigabitEthernet3/1
   1    0012.436f.c07f   dynamic ip                    GigabitEthernet3/1
   1    0050.0407.5fe1   dynamic ip                    GigabitEthernet3/1
   1    0050.6901.65af   dynamic ip                    GigabitEthernet3/1
   1    0050.da6c.81cb   dynamic ip                    GigabitEthernet3/1
   1    0050.dad0.af07   dynamic ip                    GigabitEthernet3/1
   1    00a0.ccd7.20ac   dynamic ip                    GigabitEthernet3/1
   1    00b0.64fd.1c23   dynamic ip                    GigabitEthernet3/1
   1    00b0.64fd.2d8f   dynamic assigned              GigabitEthernet3/1
   1    00d0.b775.c8bc   dynamic ip                    GigabitEthernet3/1
   1    00d0.b79e.de1d   dynamic ip                    GigabitEthernet3/1
   1    00e0.4c79.1939   dynamic ip                    GigabitEthernet3/1
   1    00e0.4c7b.d765   dynamic ip                    GigabitEthernet3/1
   1    00e0.4c82.66b7   dynamic ip                    GigabitEthernet3/1
   1    00e0.4c8b.f83e   dynamic ip                    GigabitEthernet3/1
   1    00e0.4cbc.a04f   dynamic ip                    GigabitEthernet3/1
   1    0800.20cf.8977   dynamic ip                    GigabitEthernet3/1
   1    0800.20f2.82e5   dynamic ip                    GigabitEthernet3/1
Switch#
```

This example shows how to assign MAC addresses that belong to either the “ip” or the “other” bucket to both buckets:

```
Switch(config)# mac-address-table dynamic group protocols ip other
Switch(config)# exit
Switch# show mac address-table dynamic
Unicast Entries
 vlan   mac address     type        protocols               port
-------+---------------+--------+---------------------+--------------------
   1    0000.0000.5000   dynamic ip,other              GigabitEthernet1/1
   1    0001.0234.6616   dynamic ip,other              GigabitEthernet3/1
   1    0003.4700.24c3   dynamic ip,other              GigabitEthernet3/1
   1    0003.4716.f475   dynamic ip,other              GigabitEthernet3/1
   1    0003.4748.75c5   dynamic ip,other              GigabitEthernet3/1
   1    0003.47c4.06c1   dynamic ip,other              GigabitEthernet3/1
   1    0003.47f0.d6a3   dynamic ip,other              GigabitEthernet3/1
   1    0003.47f6.a91a   dynamic ip,other              GigabitEthernet3/1
   1    0003.ba0e.24a1   dynamic ip,other              GigabitEthernet3/1
   1    0003.fd63.3eb4   dynamic ip,other              GigabitEthernet3/1
   1    0004.2326.18a1   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5d.de53   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5d.de55   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5e.6ecc   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5e.f60e   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5f.08f6   dynamic ip,other              GigabitEthernet3/1
```

```
   1    0004.5a5f.090b   dynamic ip,other             GigabitEthernet3/1
   1    0004.5a64.f813   dynamic ip,other             GigabitEthernet3/1
   1    0004.5a66.1a77   dynamic ip,other             GigabitEthernet3/1
   1    0004.5a6b.56b2   dynamic ip,other             GigabitEthernet3/1
   1    0004.5a6c.6a07   dynamic ip,other             GigabitEthernet3/1
   1    0004.5a88.b075   dynamic ip,other             GigabitEthernet3/1
   1    0004.c1bd.1b40   dynamic ip,other             GigabitEthernet3/1
   1    0004.c1d8.b3c0   dynamic ip,other             GigabitEthernet3/1
   1    0004.c1d8.bd00   dynamic ip,other             GigabitEthernet3/1
   1    0005.dce0.7c0a   dynamic assigned            GigabitEthernet3/1
   1    0007.e997.74dd   dynamic ip,other             GigabitEthernet3/1
   1    0007.e997.7e8f   dynamic ip,other             GigabitEthernet3/1
   1    0007.e9ad.5e24   dynamic ip,other             GigabitEthernet3/1
   1    0007.e9c9.0bc9   dynamic ip,other             GigabitEthernet3/1
   1    000b.5f0a.f1d8   dynamic ip,other             GigabitEthernet3/1
   1    000b.fdf3.c498   dynamic ip,other             GigabitEthernet3/1
   1    0012.436f.c07f   dynamic ip,other             GigabitEthernet3/1
   1    0050.0407.5fe1   dynamic ip,other             GigabitEthernet3/1
   1    0050.6901.65af   dynamic ip,other             GigabitEthernet3/1
   1    0050.da6c.81cb   dynamic ip,other             GigabitEthernet3/1
   1    0050.dad0.af07   dynamic ip,other             GigabitEthernet3/1
   1    00a0.ccd7.20ac   dynamic ip,other             GigabitEthernet3/1
   1    00b0.64fd.1b84   dynamic assigned            GigabitEthernet3/1
   1    00d0.b775.c8bc   dynamic ip,other             GigabitEthernet3/1
   1    00d0.b775.c8ee   dynamic ip,other             GigabitEthernet3/1
   1    00d0.b79e.de1d   dynamic ip,other             GigabitEthernet3/1
   1    00e0.4c79.1939   dynamic ip,other             GigabitEthernet3/1
   1    00e0.4c7b.d765   dynamic ip,other             GigabitEthernet3/1
   1    00e0.4c82.66b7   dynamic ip,other             GigabitEthernet3/1
   1    00e0.4c8b.f83e   dynamic ip,other             GigabitEthernet3/1
   1    00e0.4c8c.0861   dynamic ip,other             GigabitEthernet3/1
   1    0800.20d1.bf09   dynamic ip,other             GigabitEthernet3/1
Switch#
```

# mac-address-table notification

To enable MAC address notification on a switch, use the **mac-address-table notification** command. To return to the default setting, use the **no** form of this command

**mac-address-table notification** {**change** [**history-size** *hs_value*] | [**interval** *intv_value*]] | [**mac-move**] | [**threshold** [**limit** *percentage*] | [**interval** *time*]}

**no mac-address-table notification** {**change** [**history-size** *hs_value*] | [**interval** *intv_value*]] | [**mac-move**] | [**threshold** [**limit** *percentage*] | [**interval** *time*]}

## Syntax Description

| | |
|---|---|
| **change** | (Optional) Specifies enabling MAC change notification. |
| **history-size** *hs_value* | (Optional) Maximum number of entries in the MAC change notification history table. The range is 0 to 500 entries. |
| **interval** *intv_value* | (Optional) Notification trap interval, set interval time between two consecutive traps. The range is 0 to 2,147,483,647 seconds. |
| **mac-move** | (Optional) Specifies enabling MAC move notification. |
| **threshold** | (Optional) Specifies enabling MAC threshold notification. |
| **limit** *percentage* | (Optional) Specifies the percentage of MAT utilization threshold; valid values are from 1 to 100 percent. |
| **interval** *time* | (Optional) Specifies the time between MAC threshold notifications; valid values are greater than or equal to 120 seconds. |

## Defaults

MAC address notification feature is disabled.

The default MAC change trap interval value is 1 second.

The default number of entries in the history table is 1.

MAC move notification is disabled.

MAC threshold monitoring feature is disabled.

The default limit is 50 percent.

The default time is 120 seconds.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

We can enable the MAC change notification feature by using the **mac address-table notification change** command. We must also enable MAC notification traps on an interface by using the **snmp trap mac-notification change interface** configuration command and configure the switch to send MAC change traps to the NMS by using the **snmp-server enable traps mac-notification** global configuration command.

When the *history-size* option is configured, the existing MAC change history table is deleted, and a new table is created.

## Examples

This example shows how to set the MAC address notification history table size to 300 entries:

```
Switch(config)# mac-address-table notification change history-size 300
Switch(config)#
```

This example shows how to set the MAC address notification interval time to 1250 seconds:

```
Switch(config)# mac-address-table notification change interval 1250
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **clear mac-address-table** | Clears the global counter entries from the Layer 2 MAC address table. |
| **mac-address-table notification** | Enables MAC address notification on a switch. |
| **snmp-server enable traps** | Enables SNMP notifications. |
| **snmp trap mac-notification change** | Enables SNMP MAC address notifications. |

# mac-address-table static

To configure the static MAC addresses for a VLAN interface or drop unicast traffic for a MAC address for a VLAN interface, use the **mac-address-table static** command. To remove the static MAC address configurations, use the **no** form of this command.

**mac-address-table static** *mac-addr* {**vlan** *vlan-id*} {**interface** *type* | **drop**}

**no mac-address-table static** *mac-addr* {**vlan** *vlan-id*} {**interface** *type*} {**drop**}

## Syntax Description

| | |
|---|---|
| *mac-addr* | MAC address; optional when using the **no** form of this command. |
| **vlan** *vlan-id* | VLAN and valid VLAN number; valid values are from 1 to 4094. |
| **interface** *type* | Interface type and number; valid options are **FastEthernet** and **GigabitEthernet**. |
| **drop** | Drops all traffic received from and going to the configured MAC address in the specified VLAN. |

## Defaults

This command has no default settings.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(13)EW | Support for this command was introduced on the Catalyst 4500 series switches. |

## Usage Guidelines

When a static MAC address is installed, it is associated with a port.

The output interface specified must be a Layer 2 interface and not an SVI.

If you do not enter a protocol type, an entry is automatically created for each of the four protocol types.

Entering the **no** form of this command does not remove the system MAC addresses.

When removing a MAC address, entering **interface** *int* is optional. For unicast entries, the entry is removed automatically. For multicast entries, if you do not specify an interface, the entire entry is removed. You can specify the selected ports to be removed by specifying the interface.

## Examples

This example shows how to add the static entries to the MAC address table:

```
Switch(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show mac-address-table static** | Displays the static MAC address table entries only. |

# macro apply cisco-desktop

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop, use the **macro apply cisco-desktop c**ommand.

**macro apply cisco-desktop $AVID** *access_vlanid*

## Syntax Description

| | |
|---|---|
| **$AVID access_vlanid** | Specifies an access VLAN ID. |

## Defaults

This command has no default settings.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command can only be viewed and applied; it cannot be modified.

Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the macro, clear the configuration on the interface with the **default interface** command.

## Examples

This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-desktop $AVID 50
Switch(config-if)#
```

The contents of this macro are as follows:

```
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID [access_vlanid]
switchport mode access
# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
# Ensure port-security age is greater than one minute
# and use inactivity timer
# "Port-security maximum 1" is the default and will not
# Show up in the config
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

## Related Commands

| Command | Description |
|---|---|
| macro apply cisco-phone | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone. |
| macro apply cisco-router | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router. |
| macro apply cisco-switch | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch. |

# macro apply cisco-phone

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone, use the **macro apply cisco-phone** command.

**macro apply cisco-phone $AVID** ***access_vlanid*** **$VVID** ***voice_vlanid***

## Syntax Description

| | |
|---|---|
| **$AVID** ***access_vlanid*** | Specifies an access VLAN ID. |
| **$VVID** ***voice_vlanid*** | Specifies a voice VLAN ID. |

## Defaults

This command has no default settings.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command can only be viewed and applied; it cannot be modified.

Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the macro, clear the configuration on the interface with the **default interface** command.

## Examples

This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-phone $AVID 10 $VVID 50
Switch(config-if)#
```

The contents of this macro are as follows:

```
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1\
switchport access vlan $AVID [access_vlan_id]
switchport mode access
# Update the Voice VLAN (VVID) value which should be
# different from data VLAN
# Recommended value for voice vlan (VVID) should not be 1
switchport voice vlan $VVID [voice_vlan_id]
# Enable port security limiting port to a 3 MAC
# addressees -- One for desktop and two for phone
switchport port-security
switchport port-security maximum 3
# 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
# Enable auto-qos to extend trust to attached Cisco phone
auto qos voip cisco-phone
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable@
```

## Related Commands

| Command | Description |
|---|---|
| **macro apply cisco-desktop** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop. |
| **macro apply cisco-router** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router. |
| **macro apply cisco-switch** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch. |

# macro apply cisco-router

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to a router, use the **macro apply cisco-router** command.

**macro apply cisco-router $NVID** ***native_vlanid***

## Syntax Description

| | |
|---|---|
| **$NVID** ***native_vlanid*** | Specifies a native VLAN ID. |

## Defaults

This command has no default settings.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command can only be viewed and applied; it cannot be modified.

Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you applythe **macro apply cisco-router** command, clear the configuration on the interface with the **default interface** command.

## Examples

This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-router $NVID 80
Switch(config-if)#
```

The contents of this macro are as follows:

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE [vlan_range]
# Hardcode trunk and disable negotiation to
# speed up convergence
# Hardcode speed and duplex to router
switchport mode trunk
switchport nonegotiate
speed 100
duplex full
# Configure qos to trust this interface
auto qos voip trust
qos trust dscp
```

```
# Ensure fast access to the network when enabling the interface.
# Ensure that switch devices cannot become active on the interface.
spanning-tree portfast
spanning-tree bpduguard enable
```

## Related Commands

| Command | Description |
|---|---|
| **macro apply cisco-desktop** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop. |
| **macro apply cisco-phone** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone. |
| **macro apply cisco-router** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router. |
| **macro apply cisco-switch** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch. |

# macro apply cisco-switch

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch, use the **macro apply cisco-switch** command.

**macro apply cisco-switch $NVID** ***native_vlanid***

## Syntax Description

| | |
|---|---|
| **$NVID** ***native_vlanid*** | Specifies a native VLAN ID. |

## Defaults

This command has no default settings.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command can only be viewed and applied; it cannot be modified.

Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply this macro, clear the configuration on the interface with the **default interface** command.

## Examples

This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-switch $NVID 45
Switch(config-if)#
```

The contents of this macro are as follows:

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE
# Hardcode trunk and disable negotiation to
# speed up convergence
switchport mode trunk
switchport nonegotiate
# Configure qos to trust this interface
auto qos voip trust
# 802.1w defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point
```

## Related Commands

| Command | Description |
|---|---|
| **macro apply cisco-desktop** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop. |
| **macro apply cisco-phone** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone. |
| **macro apply cisco-router** | Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router. |

# macro global apply cisco-global

To apply the system-defined default template to the switch, use the **macro global apply cisco-global** global configuration command on the switch stack or on a standalone switch.

**macro global apply cisco-global**

## Syntax Description

This command has no keywords or variables.

## Defaults

This command has no default setting.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

These examples show how to apply the system-defined default to the switch:

```
Switch(config)#macro global apply cisco-global
Changing VTP domain name from gsg-vtp to [smartports] Device mode already VTP TRANSPARENT.
Switch(config)#
```

# macro global apply system-cpp

To apply the control plane policing default template to the switch, use the **macro global apply system-cpp** global configuration command on the switch stack or on a standalone switch.

**macro global apply system-cpp**

## Syntax Description

This command has no keywords or variables.

## Defaults

This command has no default setting.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

## Examples

These examples show how to apply the system-defined default to the switch:

```
Switch (config)# macro global apply system-cpp
Switch (config)#
```

## Related Commands

| Command | Description |
|---|---|
| **macro global apply cisco-global** | Applies the system-defined default template to the switch. |
| **macro global description** | Enters a description about the macros that are applied to the switch. |

# macro global description

To enter a description about the macros that are applied to the switch, use the **macro global description** global configuration command on the switch stack or on a standalone 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 mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## 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 udld aggressive mode enabled
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **macro global apply cisco-global** | Applies the system-defined default template to the switch. |

# main-cpu

To enter the main CPU submode and manually synchronize the configurations on the two supervisor engines, use the **main-cpu** command.

**main-cpu**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Redundancy

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. (Catalyst 4507R only). |

## Usage Guidelines

The main CPU submode is used to manually synchronize the configurations on the two supervisor engines. From the main CPU submode, use the **auto-sync** command to enable automatic synchronization of the configuration files in NVRAM.

**Note** After you enter the main CPU submode, you can use the **auto-sync** command to automatically synchronize the configuration between the primary and secondary route processors based on the primary configuration. In addition, you can use all of the redundancy commands that are applicable to the main CPU.

## Examples

This example shows how to reenable the default automatic synchronization feature using the auto-sync standard command to synchronize the startup-config and config-register configuration of the active supervisor engine with the standby supervisor engine. The updates for the boot variables are automatic and cannot be disabled.

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-sync standard
Switch(config-r-mc)# end
Switch# copy running-config startup-config
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| auto-sync | Enables automatic synchronization of the configuration files in NVRAM. |

# mab

To enable and configure MAC authorization bypass (MAB) on a port, use the **mab** command in interface configuration mode. To disable MAB, use the no form of this command.

**mab** [**eap**]

**no mab** [**eap**]

**Note** The **mab** command is totally independent of the effect of the **dot1x system-auth control** command.

## Syntax Description

| | |
|---|---|
| **eap** | (Optional) Specifies that a full blown EAP conversation should be used, as opposed to standard RADIUS Access-Request, Access-Accept conversation. |

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced. |

## Usage Guidelines

When a port is configured for MAB as a fallback method, it operates in a typical dot1X way until a configurable number of failed attempts to request the identity of the host. Then, the authenticator learns the MAC address of the host and uses that information to query an authentication server to see whether this MAC address will be granted access.

## Examples

The following example shows how to enable MAB on a port:

```
Switch(config-if)# mab
Switch(config-if)#
```

The following example shows how to enable and configure MAB on a port:

```
Switch(config-if)# mab eap
Switch(config-if)#
```

The following example shows how to disable MAB on a port:

```
Switch(config-if)# no mab
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show authentication** | Displays Authentication Manager information. |
| **show mab** | Displays MAB information. |
| **show running-config** | Displays the running configuration information. |

# match

To specify a match clause by selecting one or more ACLs for a VLAN access-map sequence, use the **match** subcommand. To remove the match clause, use the **no** form of this command.

**match** {**ip address** {*acl-number* | *acl-name*}} | {**mac address** *acl-name*}

**no match** {**ip address** {*acl-number* | *acl-name*}} | {**mac address** *acl-name*}

**Note** If a match clause is not specified, the action for the VLAN access-map sequence is applied to all packets. All packets are matched against that sequence in the access map.

## Syntax Description

| | |
|---|---|
| **ip address** *acl-number* | Selects one or more IP ACLs for a VLAN access-map sequence; valid values are from 1 to 199 and from 1300 to 2699. |
| **ip address** *acl-name* | Selects an IP ACL by name. |
| **mac address** *acl-name* | Selects one or more MAC ACLs for a VLAN access-map sequence. |

## Defaults

This command has no default settings.

## Command Modes

VLAN access-map

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The match clause specifies the IP or MAC ACL for traffic filtering.

The MAC sequence is not effective for IP packets. IP packets should be access controlled by IP match clauses.

Refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional configuration guidelines and restrictions.

Refer to the *Cisco IOS Command Reference* publication for additional **match** command information.

## Examples

This example shows how to define a match clause for a VLAN access map:

```
Switch(config)# vlan access-map ganymede 10
Switch(config-access-map)# match ip address 13
Switch(config-access-map)#
```

## Related Commands

| Command | Description |
|---|---|
| show vlan access-map | Displays the contents of a VLAN access map. |
| vlan access-map | Enters VLAN access-map command mode to create a VLAN access map. |

# match (class-map configuration)

To define the match criteria for a class map, use the **match** class-map configuration command. To remove the match criteria, use the **no** form of this command.

### Non-Supervisor Engine 6-E

**match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list*

**no match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list*

### Supervisor Engine 6-E and Catalyst 4900M chassis

**match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list* | **qos-group** *value* | **protocol** [**ip** | **ipv6** | **arp**]

**no match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list* | **qos-group** *value* | **protocol** [**ip** | **ipv6** | **arp**]

## Syntax Description

| | |
|---|---|
| **access-group** *acl-index-or-name* | Number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699. |
| **cos** *cos-list* | List of up to four Layer 2 class of service (CoS) values to match against a packet. Separate each value with a space. The range is 0 to 7. |
| [**lp**] **dscp** *dscp-list* | (Optional) IP keyword. It specifies that the match is for IPv4 packets only. If not used, the match is for both IPv4 and IPv6 packets.<br>List of up to eight IP Differentiated Services Code Point (DSCP) values to match against a packet. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. |
| [**lp**] **precedence** *ip-precedence-list* | (Optional) IP keyword. It specifies that the match is for IPv4 packets only. If not used, the match is for both IPv4 and IPv6 packets.<br>List of up to eight IP-precedence values to match against a packet. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. |
| **qos-group** *value* | Specifies the internally generated qos-group value assigned to a packet on the input qos classification. |
| **protocol ip** | Specifies IP in the Ethernet header. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP. |

| | |
|---|---|
| **protocol ipv6** | Specifies IPv6 in the Ethernet header. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP. |
| **protocol arp** | Specifies ARP in the Ethernet header. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 4900M chassi. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP. |

## Defaults

No match criteria are defined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switches. |
| 12.2(40)SG | Added support for the Supervisor Engine 6-E and Catalyst 4900M chassis. |
| 12.2(46)SG | Added support for the **match protocol arp** command on the Supervisor Engine 6-E and Catalyst 4900M chassis. |

## Usage Guidelines

Before entering the **match** command, you must first enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish. The **match** command is used to specify which fields in the packets are examined to classify the packets. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the quality of service (QoS) specifications set in the traffic policy.

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.

To match only IPv6 packets, you must use the **match protocol ipv6** command. To match only IPv4 packets you can use either the **ip** prefix or the protocol **ip** keyword.

To match only ARP packets, you must use the **match protocol arp** command.

You can configure the **match cos** *cos-list*, **match ip dscp** *dscp-list*, **match ip precedence** *ip-precedence-list* command in a class map within a policy map.

The **match cos** *cos-list* command applies only to Ethernet frames that carry a VLAN tag.

The **match qos-group** command is used by the class-map to identify a specific QoS group value assigned to a packet. The QoS group value is local to the switch and is associated with a packet on the input Qos classification.

Packets that do not meet any of the matching criteria are classified as members of the default traffic class. You configure it by specifying **class-default** as the class name in the **class** policy-map configuration command. For more information, see the "class" section on page 2-50.

## Examples

This example shows how to create a class map called *class2*, which matches all the inbound traffic with DSCP values of 10, 11, and 12:

```
Switch# configure terminal
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
Switch#
```

This example shows how to create a class map called *class3*, which matches all the inbound traffic with IP-precedence values of 5, 6, and 7 for both IPv4 and IPv6 traffic:

```
Switch# configure terminal
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
Switch#
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using *acl1*:

```
Switch# configure terminal
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
Switch#
```

This example shows how to specify a class-map that applies only to IPv6 traffic on a Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)# class-map match all ipv6 only
Switch(config-cmap)# match dscp af21
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch#
```

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 and to enter class-map configuration mode. |
| **show class-map** | Displays class map information. |

# match flow ip

To specify match criteria to treat flows with a unique source or destination address as new flows, use the **match flow ip** command. To disable this function, use the **no** form of this command.

**match flow ip** {**source-address** [**ip destination-address ip protocol L4 source-address L4 destination-address**] | **destination-address**}

**no match flow ip** {**source-address** [**ip destination-address ip protocol L4 source-address L4 destination-address**] | **destination-address**}

## Syntax Description

| | |
|---|---|
| **source-address** | Establishes a new flow from a flow with a unique IP source address. |
| **ip destination-address ip protocol L4 source-address L4 destination-address** | Comprises the full flow keyword; treats each flow with unique IP source, destination, protocol, and Layer 4 source and destination address as a new flow. |
| **destination-address** | Establishes a new flow from a flow with a unique IP destination address. |

## Defaults

None.

## Command Modes

class-map configuration submode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(25)SG | Support for the full flow option was added. |

## Usage Guidelines

When you specify the source-address keyword, each flow with a unique source address is treated as a new flow.

When you specify the destination-address keyword, each flow with a unique destination address is treated as a new flow.

A policy map is called a *flow-based* policy map when you configure the flow keywords on the class map that it uses. To attach a flow-based policy map as a child to an aggregate policy map, use the **service-policy** command.

**Note** The **match flow** command is available on the Catalyst 4500 series switch only when Supervisor Engine VI (WS-X4516-10GE) is present.

## Examples

This example shows how to create a flow-based class map associated with a source address:

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip source-address
Switch(config-cmap)# end
Switch#
Switch# show class-map c1
Class Map match-all c1 (id 2)
  Match flow  ip source-address
Switch#
```

This example shows how to create a flow-based class map associated with a destination address:

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# end
Switch#

Switch# show class-map c1
 Class Map match-all c1 (id 2)
   Match flow  ip destination-address
Switch#
```

Assume there are two active flows on the Fast Ethernet interface 6/1 with source addresses 192.168.10.20 and 192.168.10.21. The following example shows how to maintain each flow to 1 Mbps with an allowed burst value of 9000 bytes:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory

Switch# show policy-map interface
FastEthernet6/1

 Service-policy input: p1

   Class-map: c1 (match-all)
     15432182 packets
     Match: flow  ip source-address
     police: Per-interface
       Conform: 64995654 bytes Exceed: 2376965424 bytes

   Class-map: class-default (match-any)
     0 packets
     Match: any
       0 packets
Switch#
```

This example shows two active flows on the Fast Ethernet interface 6/1 with destination addresses of 192.168.20.20 and 192.168.20.21. The following example shows how to maintain each flow to 1 Mbps with an allowed burst value of 9000 bytes:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory

Switch# show policy-map interface
 FastEthernet6/1

  Service-policy input: p1

    Class-map: c1 (match-all)
      2965072 packets
      Match: flow  ip destination-address
      police: Per-interface
        Conform: 6105636 bytes Exceed: 476652528 bytes

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
Switch#
```

Assume there are two active flows as shown below on the Fast Ethernet interface 6/1:

```
SrcIp          DstIp          IpProt SrcL4Port DstL4Port
-------------------------------------------------------
192.168.10.10  192.168.20.20  20     6789       81
192.168.10.10  192.168.20.20  20     6789       21
```

With the following configuration, each flow is policed to a 1000000 bps with an allowed 9000-byte burst value.

**Note** If you use the **match flow ip source-address|destination-address** command, these two flows are consolidated into one flow because they have the same source and destination address.

```
Switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol l4
source-port l4 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
```

```
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1

class-map c1
   match flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port
!
 policy-map p1
    class c1
       police 1000000 bps 9000 byte conform-action transmit exceed-action drop
!
interface FastEthernet 6/1
  service-policy input p1

Switch# show class-map c1
 Class Map match-all c1 (id 2)
   Match flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port

Switch# show policy-map p1
  Policy Map p1
    Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop

Switch# show policy-map interface
 FastEthernet6/1

  Service-policy input: p1

    Class-map: c1 (match-all)
      15432182 packets
      Match: flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port
      police: Per-interface
        Conform: 64995654 bytes Exceed: 2376965424 bytes


    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| service-policy (interface configuration) | Attaches a policy map to an interface. |
| show class-map | Displays class map information. |
| show policy-map | Displays information about the policy map. |
| show policy-map interface | Displays the statistics and configurations of the input and output policies that are attached to an interface. |

# mdix auto

To enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface, use the **mdix auto** command. 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(31)SGA | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(46)SG | Added supported and unsupported linecard information to the usage guidelines. |

## Usage Guidelines

Linecards that support auto-MDIX configuration on their copper media ports include: WS-X4124-RJ45, WS-X4148-RJ with hardware revision 3.0 or later, WS-X4232-GB-RJ with hardware revision 3.0 or later, WS-X4920-GE-RJ45 and WS-4648-RJ45V+E.

Linecards that support auto-MDIX by default when port auto-negotiation enabled and cannot be turned off using an **mdix** CLI command include: WS-X4448-GB-RJ45, WS-X4548-GB-RJ45, WS-X4424-GB-RJ45, and WS-X4412-2GB-T.

Linecards that cannot support auto-MDIX functionality, either by default or CLI commands, include: WS-X4548-GB-RJ45V, WS-X4524-GB-RJ45V, WS-X4506-GB-T, WS-X4148-RJ, WS-X4248-RJ21V, WS-X4248-RJ45V, WS-X4224-RJ45V, and WS-X4232-GB-RJ.

When you enable auto-MDIX on an interface, you must also set the interface speed to be autoneogiated so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed) is enabled on one or both of connected interfaces, link up occurs even if the cable type (straight-through or crossover) is incorrect.

## Examples

This example shows how to enable auto MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface FastEthernet6/3
Switch(config-if)# speed auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **speed** | Configures the interface speed. |
| **show interfaces** | Displays traffic on a specific interface. |
| **show interfaces capabilities** | Displays the interface capabilities for an interface or for all the interfaces on a switch. |
| **show interfaces status** | Displays the interface status. |

# media-type

To select the connector for a dual-mode capable port, use the **media-type** command.

**media-type** {**rj45** | **sfp**}

## Syntax Description

| | |
|---|---|
| **rj45** | Uses the RJ-45 connector. |
| **sfp** | Uses the SFP connector. |

## Defaults

**sfp**

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(20)EWA | Support for this command was introduced for the WS-X4306-GB-T module and the WS-X4948 chassis. |

## Usage Guidelines

This command is supported on all ports on the WS-X4306-GB-T module and ports 1/45-48 on the WS-X4948 chassis.

Entering the **show interface capabilities** command provides the Multiple Media Types field, which displays the value **no** if a port is not dual-mode capable and lists the media types (**sfp** and **rj45**) for dual-mode capable ports.

## Examples

This example shows how to configure port 5/45 on a WS-X4948 chassis to use the RJ-45 connector:

```
Switch(config)# interface gigabitethernet 5/45
Switch(config-if)# media-type rj45
```

# mode

To set the redundancy mode, use the **mode** command.

**mode** {**rpr** | **sso**}

## Syntax Description

| | |
|---|---|
| **rpr** | Specifies RPR mode. |
| **sso** | Specifies SSO mode. |

## Defaults

For Catalyst 4500 series switches that are configured with Supervisor Engine II+, Supervisor Engine IV, and Supervisor Engine V, the defaults are as follows:

- SSO, if the supervisor engine is using Cisco IOS Release 12.2(20)EWA.
- RPR, if the supervisor engine is using Cisco IOS Release 12.1(12c)EW through 12.2(18)EW, as well as 12.1(*xx*)E.

**Note** If you are upgrading the current supervisor engine from Cisco IOS Release 12.2(18)EW or an earlier release to 12.2(20)EWA, and the RPR mode has been saved to the startup configuration, both supervisor engines will continue to operate in RPR mode after the software upgrade. To use SSO mode, you must manually change the redundancy mode to SSO.

## Command Modes

Redundancy configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(20)EWA | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

RPR and SSO mode are not supported on Catalyst 4500 series switches that are configured with Supervisor Engine 2.

The **mode** command can be entered only from within redundancy configuration mode.

Follow these guidelines when configuring your system to RPR or SSO mode:

- You must use identical Cisco IOS images and supervisor engines to support RPR and SSO mode. Redundancy may not work due to differences between the Cisco IOS release and supervisor engine capabilities.
- Any modules that are not online at the time of a switchover are reset and reloaded on a switchover.
- If you perform an OIR of the module within 60 seconds before a stateful switchover, the module resets during the stateful switchover and the port states are restarted.
- The FIB tables are cleared on a switchover. Routed traffic is interrupted until route tables reconverge.

The redundant supervisor engine reloads on any mode change and begins to work in the current mode.

## Examples

This example shows how to set the redundancy mode to SSO:

```
Switch(config)# redundancy
Switch(config-red)# mode sso
Switch(config-red)#
```

## Related Commands

| Command | Description |
|---|---|
| **redundancy** | Enters the redundancy configuration mode. |
| **redundancy force-switchover** | Forces a switchover from the active to the standby supervisor engine. |
| **show redundancy** | Displays redundancy facility information. |
| **show running-config** | Displays the running configuration of a switch. |

# monitor session

To enable the SPAN sessions on interfaces or VLANs, use the **monitor session** command. To remove one or more source or destination interfaces from a SPAN session, or a source VLAN from a SPAN session, use the **no** form of this command.

**monitor session** *session* {**destination interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number*} [**encapsulation** {**isl** | **dot1q**}] [**ingress** [**vlan** *vlan_id*] [**learning**]]} | {**remote vlan** *vlan_id*} | {**source** {**interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number* | **Port-channel** *interface-number*}} | [**vlan** *vlan_id*] |{**remote vlan** *vlan_id*} | {**cpu** [**queue** *queue_id* | **acl** {**input** {**error** {**rx**} | **log** {**rx**} | **punt** {**rx**} | **rx**}} | **output** {**error** {**rx**} | **forward** {**rx**} | **log** {**rx**} | **punt** {**rx**} | **rx**} | **adj-same-if** {**rx**} | **all** {**rx**} | **bridged** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4** {**rx**} | **rx**} | **control-packet** {**rx**} | **mtu-exceeded** {**rx**} | **routed** {**forward** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4** {**rx**} | **rx**} | **received** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4**{**rx**} | **rx**} | **rx**] | **rpf-failure** {**rx**} | **unknown-sa** {**rx**}]}]} [ **,** | **-** | **rx** | **tx** | **both**]} | {**filter** {**ip access-group** [**name** | **id**]}{**vlan** *vlan_id* [ **,** | **-** ]} | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} [**rx** | **tx** | **both**]}

**no monitor session** *session* {**destination interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number*} [**encapsulation** {**isl** | **dot1q**}] [**ingress** [**vlan** *vlan_id*] [**learning**]]} | {**remote vlan** *vlan_id*} | {**source** {**interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number* | **Port-channel** *interface-number*}} | [**vlan** *vlan_id*] |{**remote vlan** *vlan_id*} | {**cpu** [**queue** *queue_id* | **acl** {**input** {**error** {**rx**} | **log** {**rx**} | **punt** {**rx**} | **rx**}} | **output** {**error** {**rx**} | **forward** {**rx**} | **log** {**rx**} | **punt** {**rx**} | **rx**} | **adj-same-if** {**rx**} | **all** {**rx**} | **bridged** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4** {**rx**} | **rx**} | **control-packet** {**rx**} | **mtu-exceeded** {**rx**} | **routed** {**forward** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4** {**rx**} | **rx**} | **received** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4**{**rx**} | **rx**} | **rx**] | **rpf-failure** {**rx**} | **unknown-sa** {**rx**}]}]} [ **,** | **-** | **rx** | **tx** | **both**]} | {**filter** {**ip access-group** [**name** | **id**]}{**vlan** *vlan_id* [ **,** | **-** ]} | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} [**rx** | **tx** | **both**]}

### Supervisor Engine 6-E and Catalyst 4900M chassis

**monitor session** *session* {**destination interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number*} [**encapsulation** {**isl** | **dot1q**}] [**ingress** [**vlan** *vlan_id*] [**learning**]]} | {**remote vlan** *vlan_id*} | {**source** { **interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number* | **Port-channel** *interface-number*}} | [**vlan** *vlan_id*] |{**remote vlan** *vlan_id*} | {**cpu** [**queue** *queue_id* | **acl** { **input** {**copy** {**rx**} | **error** {**rx**} | **forward** {**rx**} | **punt** {**rx**} | **rx**} } | **output** {**copy** {**rx**} | **error** {**rx**} | **forward** {**rx**} | **punt** {**rx**} | **rx**} | **all** {**rx**} | **control-packet** {**rx**} | **esmp** {**rx**} | **l2-forward** { **adj-same-if** {**rx**} | **bridge-cpu** {**rx**} | **ip-option** {**rx**} | **ipv6-scope-check-fail** {**rx**} | **l2-src-index-check-fail** {**rx**} | **mcast-rpf-fail** {**rx**} | **non-arpa** {**rx**} | **router-cpu** {**rx**} | **ttl-expired** {**rx**} | **ucast-rpf-fail** {**rx**} | **rx**} | **l3-forward** { **forward** {**rx**} | **glean** {**rx**} | **receive** {**rx**} | **rx**} **mtu-exceeded** {**rx**} | **unknown-port-vlan-mapping** {**rx**} | **unknown-sa** {**rx**}]} [ **,** | **-** | **rx** | **tx** | **both**]} | {**filter** {**ip access-group** [**name** | **id**]}{**vlan** *vlan_id* [ **,** | **-** ]} | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} [**rx** | **tx** | **both**]}

**no monitor session** *session* {**destination interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number*} [**encapsulation** {**isl** | **dot1q**}] [**ingress** [**vlan** *vlan_id*] [**learning**]]} | {**remote vlan** *vlan_id*} | {**source** {**cpu**{**both** | **queue** | **rx** | **tx**} | **interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number* | **Port-channel** *interface-number*}} | [**vlan** *vlan_id*] |{**remote vlan** *vlan_id*} | {**cpu** [**queue** *queue_id* | **acl** {**input** {**copy** {**rx**} | **error** {**rx**} | **forward** {**rx**} | **punt** {**rx**} | **rx**} } | **output** {**copy** {**rx**} | **error** {**rx**} | **forward** {**rx**} | **punt** {**rx**} | **rx**} | **all** {**rx**} | **control-packet** {**rx**} | **esmp** {**rx**} | **l2-forward**

{ **adj-same-if** {rx} | **bridge-cpu** {**rx**} | **ip-option** {**rx**} | **ipv6-scope-check-fail** {**rx**} | **l2-src-index-check-fail** {**rx**} | **mcast-rpf-fail** {**rx**} | **non-arpa** {**rx**} | **router-cpu** {**rx**} | **ttl-expired** {**rx**} | **ucast-rpf-fail** {**rx**} | **rx**} | **l3-forward** {**forward** {**rx**} | **glean** {**rx**} | **receive** {**rx**} | **rx**} **mtu-exceeded** {**rx**} | **unknown-port-vlan-mapping** {**rx**} | **unknown-sa** {**rx**}]} [ **,** | **-** | **rx** | **tx** | **both**]} | {**filter** {**ip access-group** [**name** | **id**]}{**vlan** *vlan_id* [ **,** | **-** ]} | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} [**rx** | **tx** | **both**]}

## Syntax Description

| | |
|---|---|
| *session* | Number of a SPAN session; valid values are from 1 to 6. |
| **destination** | Specifies a SPAN destination. |
| **interface** | Specifies an interface. |
| **FastEthernet** *interface-number* | Specifies a Fast Ethernet module and port number; valid values are from 1 to 6. |
| **GigabitEthernet** *interface-number* | Specifies a Gigabit Ethernet module and port number; valid values are from 1 to 6. |
| **encapsulation** | (Optional) Specifies the encapsulation type of the destination port. |
| **isl** | (Optional) Specifies ISL encapsulation. |
| **dot1q** | (Optional) Specifies dot1q encapsulation. |
| **ingress** | (Optional) Indicates whether the ingress option is enabled. |
| **vlan** *vlan_id* | (Optional) Specifies the VLAN; valid values are from 1 to 4094. |
| **learning** | (Optional) Enables host learning on ingress-enabled destination ports. |
| **remote vlan** *vlan_id* | Specifies an RSPAN source or destination session on a switch. |
| **source** | Specifies a SPAN source. |
| **Port-channel** *interface-number* | Specifies a port-channel interface; valid values are from 1 to 64. |
| **cpu** | Causes traffic received or sent from the CPU to be copied to the destination of the session. |
| **queue** *queue_id* | (Optional) Specifies that only traffic received on the specific CPU subqueue should be copied to the destination of the session. Valid values are from 1 to 64, or by the following names: all, control-packet, esmp, mtu-exceeded, unknown-port-vlan-mapping, unknown-sa, acl input, acl input copy, acl input error, acl input forward, acl input punt, acl output, acl output copy, acl output error, acl output forward, acl output punt, l2-forward, adj-same-if, bridge-cpu, ip-option, ipv6-scope-check-fail, l2-src-index-check-fail, mcast-rpf-fail, non-arpa, router-cpu, ttl-expired, ucast-rpf-fail, l3-forward, forward, glean, receive. |
| **acl** | (Optional) Specifies input and output ACLs; valid values are from 14 to 20. |
| **input** | Specifies input ACLs; valid values are from 14 to 16. |
| **error** | Specifies the ACL software errors. |
| **log/copy** | Specifies packets for ACL logging. |
| **punt** | Specifies packets punted due to overflows. |
| **rx** | Specifies monitoring received traffic only. |

| | |
|---|---|
| **output** | Specifies output ACLs; valid values are from 17 to 20. |
| **l2-forward** | (Optional) Layer 2 or Layer 3 exception packets. |
| **bridge-cpu** | Specifies packets bridged to CPU. |
| **ip-option** | Specifies packets with an IP option. |
| **ipv6-scope-check-fail** | Specifies IPv6 packets with scope-check failures. |
| **l2-src-index-check-fail** | Specifies IP packets with mismatched SRC MAC and SRC IP addresses. |
| **mcast-rpf-fail** | Specifies IPv4/IPv6 multicast RPF failures. |
| **non-arpa** | Specifies packets with non-ARPA encapsulation. |
| **router-cpu** | Specifies software routed packets. |
| **ttl-expired** | Specifies IPv4 routed pacekts exceed TTL. |
| **adj-same-if** | Specifies packets routed to the incoming interface. |
| **bridged** | Specifies Layer 2 bridged packets. |
| **1** | Specifies packets with the highest priority. |
| **2** | Specifies packets with the a high priority. |
| **3** | Specifies packets with the a medium priority. |
| **4** | Specifies packets with the a low priority. |
| **ucast-rpf-fail** | Specifies IPv4/IPv6 Unicast RPF failures. |
| **all** | (Optional) all queues. |
| **l3-forward** | (Optional) Layer 3 packets. |
| **forward** | Specifies special Layer 3 forwards tunnel encapsulation. |
| **glean** | Specifies special Layer 3 forwards glean. |
| **receive** | Specifies packets addressed to a port. |
| **control-packet** | (Optional) Layer 2 control packets. |
| **esmp** | (Optional) ESMP packets. |
| **mtu-exceeded** | (Optional) Output Layer 3 interface MTU exceeded. |
| **routed** | Specifies Layer 3 routed packets. |
| **received** | Specifies packets addressed to a port. |
| **rpf-failure** | Specifies Multicast RPF failed packets. |
| **unknown-port-vlan-mapping** | (Optional) Packets with missing port-VLAN mapping. |
| **unknown-sa** | (Optional) Packets with missing source-IP-addresses. |
| **,** | (Optional) Symbol to specify another range of SPAN VLANs; valid values are from 1 to 4094. |
| **-** | (Optional) Symbol to specify a range of SPAN VLANs. |
| **both** | (Optional) Monitors and filters received and transmitted traffic. |
| **rx** | (Optional) Monitors and filters received traffic only. |
| **tx** | (Optional) Monitors and filters transmitted traffic only. |
| **filter** | Limits SPAN source traffic to specific VLANs. |
| **ip access-group** | (Optional) Specifies an IP access group filter, either a name or a number. |
| **name** | (Optional) Specifies an IP access list name. |

| | |
|---|---|
| **id** | (Optional) Specifies an IP access list number. Valid values are 1 to 199 for an IP access list and 1300 to 2699 for an IP expanded access list. |
| **vlan** *vlan_id* | (Optional) Specifies the VLAN to be filtered. The number is entered as a single value or a range; valid values are from 1 to 4094. |
| **packet-type** | Limits SPAN source traffic to packets of a specified type. |
| **good** | Specifies a good packet type |
| **bad** | Specifies a bad packet type. |
| **address-type unicast \| multicast \| broadcast** | Limits SPAN source traffic to packets of a specified address type. Valid types are unicast, multicast, and broadcast. |

## Defaults

Received and transmitted traffic, as well as all VLANs, packet types, and address types are monitored on a trunking interface.

Packets are transmitted untagged out the destination port; ingress and learning are disabled.

All packets are permitted and forwarded "as is" on the destination port.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(11b)EW | Support for differing directions within a single-user session and extended VLAN addressing was added. |
| 12.1(19)EW | Support for ingress packets, encapsulation specification, packet and address type filtering, and CPU source sniffing enhancements was added. |
| 12.1(20)EW | Support for remote SPAN and host learning on ingress-enabled destination ports was added. |
| 12.2(20)EW | Support for an IP access group filter was added. |
| 12.2(40)SG | Support for Supervisor Engine 6-E and Catalyst 4900M chassis CPU queue options was added. |

## Usage Guidelines

Only one SPAN destination for a SPAN session is supported. If you attempt to add another destination interface to a session that already has a destination interface that is configured, you will get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

Beginning in Cisco IOS Release 12.1(12c)EW, you can configure sources from different directions within a single user session.

**Note** Beginning in Cisco IOS Release 12.1(12c)EW, SPAN is limited to two sessions containing ingress sources and four sessions containing egress sources. Bidirectional sources support both ingress and egress sources.

A particular SPAN session can either monitor VLANs or monitor individual interfaces: you cannot have a SPAN session that monitors both specific interfaces and specific VLANs. If you first configure a SPAN session with a source interface, and then try to add a source VLAN to the same SPAN session, you will receive an error. You will also receive an error message if you configure a SPAN session with a source VLAN, and then try to add a source interface to that session. You must first clear any sources for a SPAN session before switching to another type of source. CPU sources may be combined with source interfaces and source VLANs.

When configuring the **ingress** option on a destination port, you must specify an ingress VLAN if the configured encapsulation type is untagged (the default) or is 802.1Q. If the encapsulation type is ISL, then no ingress VLAN specification is necessary.

By default, when you enable ingress, no host learning is performed on destination ports. When you enter the **learning** keyword, host learning is performed on the destination port, and traffic to learned hosts is forwarded out the destination port.

If you enter the **filter** keyword on a monitored trunking interface, only traffic on the set of specified VLANs is monitored. Port-channel interfaces are displayed in the list of **interface** options if you have them configured. VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session** *session* **source vlan** *vlan-id* command.

The packet-type filters are supported only in the Rx direction. You can specify both Rx- and Tx-type filters and multiple-type filters at the same time (for example, you can use **good** and **unicast** to only sniff nonerror unicast frames). As with VLAN filters, if you do not specify the type, the session will sniff all packet types.

The **queue** identifier allows sniffing for only traffic that is sent or received on the specified CPU queues. The queues may be identified either by number or by name. The queue names may contain multiple numbered queues for convenience.

## Examples

This example shows how to configure IP access group 100 on a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 filter ip access-group 100
Switch(config)# end
Switch(config)#
```

This example shows how to add a source interface to a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface fa2/3
Switch(config)# end
Switch(config)#
Switch(config)#
Switch(config)#
```

This example shows how to configure the sources with different directions within a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)# end
```

This example shows how to remove a source interface from a SPAN session:

```
Switch# configure terminal
Switch(config)# no monitor session 1 source interface fa2/3
Switch(config)# end
```

This example shows how to limit SPAN traffic to VLANs 100 through 304:

```
Switch# configure terminal
Switch(config)# monitor session 1 filter vlan 100 - 304
Switch(config)# end
```

This example shows how to configure RSPAN VLAN 20 as the destination:

```
Switch# configure terminal
Switch(config)# monitor session 2 destination remote vlan 20
Switch(config)# end
```

This example shows how to use queue names and queue number ranges for the CPU as a SPAN source on Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 3 source cpu queue 10 rx
Switch(config)# end
```

**Note** For Supervisor Engine 6-E, control-packet is mapped to queue 10.

## Related Commands

| Command | Description |
|---|---|
| show monitor | Displays information about the SPAN session. |

# mtu

To enable jumbo frames on an interface by adjusting the maximum size of a packet or maximum transmission unit (MTU), use the **mtu** command. To return to the default setting, use the **no** form of this command.

**mtu** *bytes*

**no mtu**

## Syntax Description

| | |
|---|---|
| *bytes* | Byte size; valid values are from 1500 to 9198. |

## Defaults

The default settings are as follows:

- Jumbo frames are disabled
- 1500 bytes for all ports

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(13)EW | Support for this command was introduced on the Catalyst 4500 series switches. |

## Usage Guidelines

Jumbo frames are supported on nonblocking Gigabit Ethernet ports, switch virtual interfaces (SVI), and EtherChannels. Jumbo frames are not available for stub-based ports.

The baby giants feature uses the global **system mtu** *size* command to set the global baby giant MTU. It allows all stub-based port interfaces to support an Ethernet payload size of up to 1552 bytes.

Both the **system mtu** command and the per-interface **mtu** command work on interfaces that can support jumbo frames, but the per-interface **mtu** command takes precedence.

## Examples

This example shows how to specify an MTU of 1800 bytes:

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# mtu 1800
```

## Related Commands

| Command | Description |
|---|---|
| system mtu | Sets the maximum Layer 2 or Layer 3 payload size. |

# name

To set the MST region name, use the **name** command. To return to the default name, use the **no** form of this command.

**name** *name*

**no name** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the MST region. The name can be any string with a maximum length of 32 characters. |

## Defaults

The MST region name is not set.

## Command Modes

MST configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Two or more Catalyst 4500 series switches with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

## Examples

This example shows how to name a region:

```
Switch(config-mst)# name Cisco
Switch(config-mst)#
```

## Related Commands

| Command | Description |
|---|---|
| **instance** | Maps a VLAN or a set of VLANs to an MST instance. |
| **revision** | Sets the MST configuration revision number. |
| **show spanning-tree mst** | Displays MST protocol information. |
| **spanning-tree mst configuration** | Enters the MST configuration submode. |

# pagp learn-method

To learn the input interface of the incoming packets, use the **pagp learn-method** command. To return to the default value, use the **no** form of this command.

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

**no pagp learn-method**

## Syntax Description

| | |
|---|---|
| **aggregation-port** | Specifies learning the address on the port channel. |
| **physical-port** | Specifies learning the address on the physical port within the bundle. |

## Defaults

Aggregation port is enabled.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to enable physical port address learning within the bundle:

```
Switch(config-if)# pagp learn-method physical-port
Switch(config-if)#
```

This example shows how to enable aggregation port address learning within the bundle:

```
Switch(config-if)# pagp learn-method aggregation-port
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show pagp** | Displays information about the port channel. |

# pagp port-priority

To select a port in hot standby mode, use the **pagp port-priority** command. To return to the default value, use the **no** form of this command.

**pagp port-priority** *priority*

**no pagp port-priority**

## Syntax Description

| | |
|---|---|
| *priority* | Port priority number; valid values are from 1 to 255. |

## Defaults

Port priority is set to 128.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The higher the priority, the better the chances are that the port will be selected in the hot standby mode.

## Examples

This example shows how to set the port priority:

```
Switch(config-if)# pagp port-priority 45
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **pagp learn-method** | Learns the input interface of the incoming packets. |
| **show pagp** | Displays information about the port channel. |

# passive-interface

To disable sending routing updates on an interface, use the **passive-interface** command. To reenable the sending of routing updates, use the **no** form of this command.

**passive-interface** [[**default**] {*interface-type interface-number*}] | {**range** *interface-type interface-number-interface-type interface-number*}

**no passive-interface** [[**default**] {*interface-type interface-number*}] | {**range** *interface-type interface-number-interface-type interface-number*}

## Syntax Description

| | |
|---|---|
| **default** | (Optional) All interfaces become passive. |
| *interface-type* | Specifies the interface type. |
| *interface-number* | Specifies the interface number. |
| **range** range | Specifies the range of subinterfaces being configured; see the "Usage Guidelines" section. |

## Defaults

Routing updates are sent on the interface.

## Command Modes

Router configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You can use the **passive-interface range** command on the following interfaces: FastEthernet, GigabitEthernet, VLAN, Loopback, Port-channel, 10-GigabitEthernet, and Tunnel. When you use the **passive-interface range** command on a VLAN interface, the interface should be the existing VLAN SVIs. To display the VLAN SVIs, enter the **show running config** command. The VLANs that are not displayed cannot be used in the **passive-interface range** command.

The values that are entered with the **passive-interface range** command are applied to all the existing VLAN SVIs.

Before you can use a macro, you must define a range using the **define interface-range** command.

All configuration changes that are made to a port range through the **passive-interface range** command are retained in the running-configuration as individual passive-interface commands.

You can enter the **range** in two ways:

- Specifying up to five interface ranges
- Specifying a previously defined macro

You can either specify the interfaces or the name of an interface-range macro. An interface range must consist of the same interface type, and the interfaces within a range cannot span across the modules.

You can define up to five interface ranges on a single command; separate each range with a comma:

**interface range gigabitethernet 5/1-20, gigabitethernet4/5-20.**

Use this format when entering the *port-range*:

- *interface-type* {*mod*}/{*first-port*} - {*last-port*}

You cannot specify both a macro and an interface range in the same command. After creating a macro, you can enter additional ranges. If you have already entered an interface range, the CLI does not allow you to enter a macro.

You can specify a single interface in the **range** *range* value. This makes the command similar to the **passive-interface** *interface-number* command.

**Note** The **range** keyword is only supported in OSPF, EIGRP, RIP, and ISIS router mode.

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

For the Open Shortest Path First (OSPF) protocol, OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

**Note** For IS-IS you must keep at least one active interface and configure the interface with the **ip router isis** command.

Enhanced Interior Gateway Routing Protocol (EIGRP) is disabled on an interface that is configured as passive although it advertises the route.

## Examples

The following example sends EIGRP updates to all interfaces on network 10.108.0.0 except GigabitEthernet interface 1/1:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# router eigrp 109
Switch(config-router)# network 10.108.0.0
Switch(config-router)# passive-interface gigabitethernet 1/1
Switch(config-router)#
```

The following configuration enables IS-IS on Ethernet interface 1 and serial interface 0 and advertises the IP addresses of Ethernet interface 0 in its link-state protocol data units (PDUs):

```
Switch(config-if)# router isis Finance
Switch(config-router)# passive-interface Ethernet 0
Switch(config-router)# interface Ethernet 1
Switch(config-router)# ip router isis Finance
Switch(config-router)# interface serial 0
Switch(config-router)# ip router isis Finance
Switch(config-router)#
```

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface default
Switch(config-router)# no passive-interface ethernet0
Switch(config-router)# network 10.108.0.1 0.0.0.255 area 0
Switch(config-router)#
```

The following configuration sets the Ethernet ports 3 through 4 on module 0 and GigabitEthernet ports 4 through 7 on module 1 as passive:

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface range ethernet0/3-4,gigabitethernet1/4-7
Switch(config-router)#
```

# permit

To permit an ARP packet based on matches against the DHCP bindings, use the **permit** command. To remove a specified ACE from an access list, use the **no** form of this command

**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**]

## Syntax Description

| | |
|---|---|
| **request** | (Optional) Requests a match for the ARP request. When **request** is not specified, matching is performed against all ARP packets. |
| **ip** | Specifies the sender IP address. |
| **any** | Specifies that any IP or MAC address will be accepted. |
| **host** *sender-ip* | Specifies that only a specific sender IP address will be accepted. |
| *sender-ip sender-ip-mask* | Specifies that a specific range of sender IP addresses will be accepted. |
| **mac** | Specifies the sender MAC address. |
| **host** *sender-mac* | Specifies that only a specific sender MAC address will be accepted. |
| *sender-mac sender-mac-mask* | Specifies that a specific range of sender MAC addresses will be accepted. |
| **response** | Specifies a match for the ARP responses. |
| **ip** | Specifies the IP address values for the ARP responses. |
| **host** *target-ip* | (Optional) Specifies that only a specific target IP address will be accepted. |
| *target-ip target-ip-mask* | (Optional) Specifies that a specific range of target IP addresses will be accepted. |
| **mac** | Specifies the MAC address values for the ARP responses. |
| **host** *target-mac* | (Optional) Specifies that only a specific target MAC address will be accepted. |
| *target-mac target-mac-mask* | (Optional) Specifies that a specific range of target MAC addresses will be accepted. |
| **log** | (Optional) Logs a packet when it matches the access control entry (ACE). |

## Defaults

This command has no default settings.

## Command Modes

arp-nacl configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Permit clauses can be added to forward or drop ARP packets based on some matching criteria.

## Examples

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

```
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
Switch# show arp access-list

ARP access list static-hosts
    permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| arp access-list | Defines an ARP access list or adds clauses at the end of a predefined list. |
| deny | Denies an ARP packet based on matches against the DHCP bindings. |
| ip arp inspection filter vlan | Permits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and applies it to a VLAN. |

# police

To configure the Traffic Policing feature, use the **police** QoS policy-map class configuration command. To remove the Traffic Policing feature from the configuration, use the **no** form of this command.

**police** {*bps* | *kbps* | *mbps* |*gbps*} [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

**no police** {*bps* | *kbps* | *mbps* |*gbps*} [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

## Syntax Description

| | |
|---|---|
| *bps* | Average rate, in bits per second. Valid values are 32,000 to 32,000,000,000. |
| *kbps* | Average rate, in kilobytes per second. Valid values are 32 to 32,000,000. |
| *mbps* | Average rate, in megabits per second. Valid values are 1 to 32,000. |
| *gbps* | Average rate, in gigabits per second. Valid values are 1 to 32. |
| *burst-normal* | (Optional) Normal burst size, in bytes. Valid values are 64 to 2,596,929,536. Burst value of up to four times the configured rate can be supported. |
| *burst-max* | (Optional) Excess burst size, in bytes. Valid values are 64 to 2,596,929,536. Burst value of upto four times the configured rate can be supported. |
| **conform-action** | Action to take on packets that conform to the rate limit. |
| **exceed-action** | Action to take on packets that exceed the rate limit. |
| **violate-action** | (Optional) Action to take on packets that violate the normal and maximum burst sizes. |
| *action* | Action to take on packets. Specify one of the following keywords:<br>• **drop**—Drops the packet.<br>• **set-cos-transmit** new-ios—Set the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.<br>• **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting.<br>• **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value setting.<br>• **transmit**—Transmits the packet. The packet is not altered. |

## Defaults

This command is disabled by default.

## Command Modes

Policy-map class configuration (when specifying a single action to be applied to a market packet)

Policy-map class police configuration (when specifying multiple actions to be applied to a marked packet)

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E. |

## Usage Guidelines

Use the **police** command to mark a packet with different quality of service (QoS) values based on conformance to the service-level agreement.

Traffic policing will not be executed for traffic that passes through an interface.

### Specifying Multiple Actions

The **police** command allows you to specify multiple policing actions. When specifying multiple policing actions when configuring the **police** command, note the following points:

- You can specify a maximum of four actions at one time.
- You cannot specify contradictory actions such as **conform-action** *transmit* and **conform-action** *drop*.

### Using the Police Command with the Traffic Policing Feature

The **police** command can be used with Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are a single-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the **violate-action** option is not specified, and a two-token bucket system is used when the **violate-action** option is specified.

### Token Bucket Algorithm with One Token Bucket

The one token bucket algorithm is used when the **violate-action** option is not specified in the **police** command of the command-line interface (CLI).

The conform bucket is initially set to the full size (the full size is the number of bytes specified as the normal burst size).

When a packet of a given size (for example, “B” bytes) arrives at specific time (time “T”) the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time is T, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The token arrival rate is calculated as follows:

  (time between packets <which is equal to T - T1> * policer rate)/8 bytes
- If the number of bytes in the conform bucket B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.
- If the number of bytes in the conform bucket B (minus the packet size to be limited) is fewer than 0, the exceed action is taken.

#### Token Bucket Algorithm with Two Token Buckets (Refer to RFC 2697)

The two-token bucket algorithm is used when the **violate-action** is specified in the **police** command CLI.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, “B” bytes) arrives at specific time (time “T”) the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at t, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

  The token arrival rate is calculated as follows:

  (time between packets <which is equal to T-T1> * policer rate)/8 bytes
- If the number of bytes in the conform bucket - B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in the conform bucket B is less than 0, the excess token bucket is checked for bytes by the packet. If the number of bytes in the exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

## Examples

#### Token Bucket Algorithm with One Token Bucket

This example shows how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the Traffic Policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, Traffic Policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets leaving Gigabit Ethernet interface 6/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output police-setting
Switch(config-if)# end
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the token bucket ((0.25 * 8000)/8), leaving 800 bytes in the token bucket. If the next packet is 900 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

#### Token Bucket Algorithm with Two Token Buckets Example (Refer to RFC 2697)

In this particular example, Traffic Policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Gigabit Ethernet interface 6/1.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1
violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output police-setting
Switch(config-if)# end
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket ((0.25 * 8000)/8), leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size) is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket.

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets ((.40 * 8000)/8). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 bytes overflow the conform token bucket (because it only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket ((.20 * 8000)/8). Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

## Related Commands

| Command | Description |
|---|---|
| **police (percent)** | Configures traffic policing on the basis of a percentage of bandwidth available on an interface. |
| **police (two rates)** | Configures traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR). |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **service-policy (policy-map class)** | Creates a service policy that is a quality of service (QoS) policy within a policy map. |
| **show policy-map** | Displays information about the policy map. |
| **show policy-map interface** | Displays the statistics and configurations of the input and output policies that are attached to an interface. |

# police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in QoS policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

**police cir percent** *percent* [**bc** *conform-burst-in-msec*] [**pir percent** *percentage*] [**be** *peak-burst-inmsec*]

**no police cir percent** *percent* [**bc** *conform-burst-in-msec*] [**pir percent** *percentage*] [**be** *peak-burst-inmsec*]

## Syntax Description

| | |
|---|---|
| **cir** | Committed information rate. Indicates that the CIR will be used for policing traffic. |
| **percent** | Specifies that a percentage of bandwidth will be used for calculating the CIR. |
| *percent* | Specifies the bandwidth percentage. Valid range is a number from 1 to 100. |
| **bc** | (Optional) Conform burst (bc) size used by the first token bucket for policing traffic. |
| *conform-burst-in-msec* | (Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000. |
| **pir** | (Optional) Peak information rate (PIR). Indicates that the PIR will be used for policing traffic. |
| **percent** | (Optional) Specifies that a percentage of bandwidth will be used for calculating the PIR. |
| *percent* | (Optional) Specifies the bandwidth percentage. Valid range is a number from 1 to 100. |
| **be** | (Optional) Peak burst (be) size used by the second token bucket for policing traffic. |
| *peak-burst-in-msec* | (Optional) Specifies the be size in milliseconds. Valid range is a number from 1 to 2000. |
| *action* | Action to take on packets. Specify one of the following keywords:<br>• **drop**—Drops the packet.<br>• **set-cos-transmit** new-ios—Set the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.<br>• **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting.<br>• **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value setting.<br>• **transmit**—Transmits the packet. The packet is not altered. |

## Command Default

This command is disabled by default.

**Command Modes**

Policy-map class configuration

**Command History**

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E. |

**Usage Guidelines**

This command calculates the cir and pir on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent cir and pir values in bits per second (bps) are calculated on the basis of the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the bps rate calculated.

The calculated cir and pir bps rates must be in the range of 32,000 and 32,000,000,000 bps. If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the cir and the pir are recalculated on the basis of the revised amount of bandwidth. If the cir and pir percentages are changed after the policy map is attached to the interface, the bps values of the cir and pir are recalculated.

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

**Examples**

This example shows how to configure traffic policing using a CIR and a PIR based on a percentage of bandwidth on Gigabit interface 6/2. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class-map class1
Switch(config-pmap-c)# police cir percent 20 bc 3 ms pir percent 40 be 4 ms
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# interface gigabitethernet 6/2
Switch(config-if)# service-policy output policy
Switch(config-if)# end
```

# police rate

To configure single or dual rate policer, use the **police rate** command in policy-map configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

### Syntax for Bytes Per Second

**police rate** *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**pack-burst** *peak-burst-in-bytes* **bytes**]

**no police rate** *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**pack-burst** *peak-burst-in-bytes* **bytes**]

### Syntax for Percent

**police rate percent** *percentage* [**burst** *ms* **ms**] [**peak-rate** *percent* **percentage**] [**pack-burst** *ms* **ms**]

**no police rate percent** *percentage* [**burst** *ms* **ms**] [**peak-rate** *percent* **percentage**] [**pack-burst** *ms* **ms**]

## Syntax Description

| | |
|---|---|
| *units* | Specifies the traffic police rate in bits per second. Valid range is 32,000 to 32,000,000,000. |
| **bps** | (Optional) Bits per second (bps) will be used to determine the rate at which traffic is policed.<br><br>**Note** If a rate is not specified, traffic is policed via bps. |
| **burst** *burst-in-bytes* **bytes** | (Optional) Specifies the burst rate, in bytes, will be used for policing traffic. Valid range is from 64 to 2,596,929,536. |
| **peak-rate** *peak-rate-in-bps* **bps** | (Optional) Specifies the peak burst value, in bytes, for the peak rate. Valid range is from 32,000 to 32,000,000,000. |
| **peak-burst** *peak-burst-in-bytes* **bytes** | (Optional) Specifies the peak burst value, in bytes, will be used for policing traffic. If the police rate is specified in bps, the valid range of values is 64 to 2,596,929,536. |
| **percent** | (Optional) A percentage of interface bandwidth will be used to determine the rate at which traffic is policed. |
| *percentage* | (Optional) Bandwidth percentage. Valid range is a number from 1 to 100. |
| **burst** *ms* **ms** | (Optional) Burst rate, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000. |
| **peak-rate percent** *percentage* | (Optional) A percentage of interface bandwidth will be used to determine the PIR. Valid range is a number from 1 to 100. |
| **peak-burst** *ms* **ms** | (Optional) Peak burst rate, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000. |

## Command Default

This command is disabled by default.

## Command Modes

Policy-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E. |

## Usage Guidelines

Use the **police rate** command to limit traffic on the basis of pps, bps, or a percentage of interface bandwidth.

If the **police rate** command is issued, but the a rate is not specified, traffic that is destined will be policed on the basis of bps.

## Examples

This example shows how to configure policing on a class to limit traffic to an average rate of 1,500,000 bps:

```
Switch(config)# class-map c1
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police rate 1500000  burst 500000
Switch(config-pmap-c)# exit
```

## Related Commands

| Command | Description |
|---|---|
| policy-map | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| show policy-map | Displays information about the policy map. |

# police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

**police cir** *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**no police cir** *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

## Syntax Description

| | |
|---|---|
| **cir** | Committed information rate (CIR) at which the first token bucket is updated. |
| *cir* | Specifies the CIR value in bits per second. The value is a number from 32,000 to 32,000,000,000. |
| **bc** | (Optional) Conform burst (bc) size used by the first token bucket for policing. |
| *conform-burst* | (Optional) Specifies the bc value in bytes. The value is a number from 64 to 2,596,929,536. |
| **pir** | Peak information rate (PIR) at which the second token bucket is updated. |
| *pir* | Specifies the PIR value in bits per second. The value is a number from 32,000 to 32,000,000,000. |
| **be** | (Optional) Peak burst (be) size used by the second token bucket for policing. |
| *peak-burst* | (Optional) Specifies the peak burst (be) size in bytes. The value is a number from 64 to 2,596,929,536. |
| **conform-action** | (Optional) Action to take on packets that conform to the CIR and PIR. |
| **exceed-action** | (Optional) Action to take on packets that conform to the PIR but not the CIR. |
| **violate-action** | (Optional) Action to take on packets exceed the PIR. |
| *action* | (Optional) Action to take on packets. Specify one of the following keywords:<br>• **drop**—Drops the packet.<br>• **set-cos-transmit** new-ios—Set the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.<br>• **set-dscp-transmit** *new-dscp*—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.<br>• **set-prec-transmit** *new-prec*—Sets the IP precedence and sends the packet with the new IP precedence value setting.<br>• **transmit**—Sends the packet with no alteration. |

## Command Default

This command is disabled by default.

## Command Modes

Policy-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E. |

## Usage Guidelines

Refer to RFC 2698-Two Rate Three Color Marker.

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the two-rate policer. The Tc token bucket can contain up to the confirm burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

### Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

Tc(t) = min(CIR * (t-t1) + Tc(t1), Bc)

Tp(t) = min(PIR * (t-t1) + Tp(t1), Be)

### Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

- If B > Tp(t), the packet is marked as violating the specified rate.
- If B > Tc(t), the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as Tp(t) = Tp(t) – B.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets—Tc(t) and Tp(t)—are updated as follows:

Tp(t) = Tp(t) – B

Tc(t) = Tc(t) – B

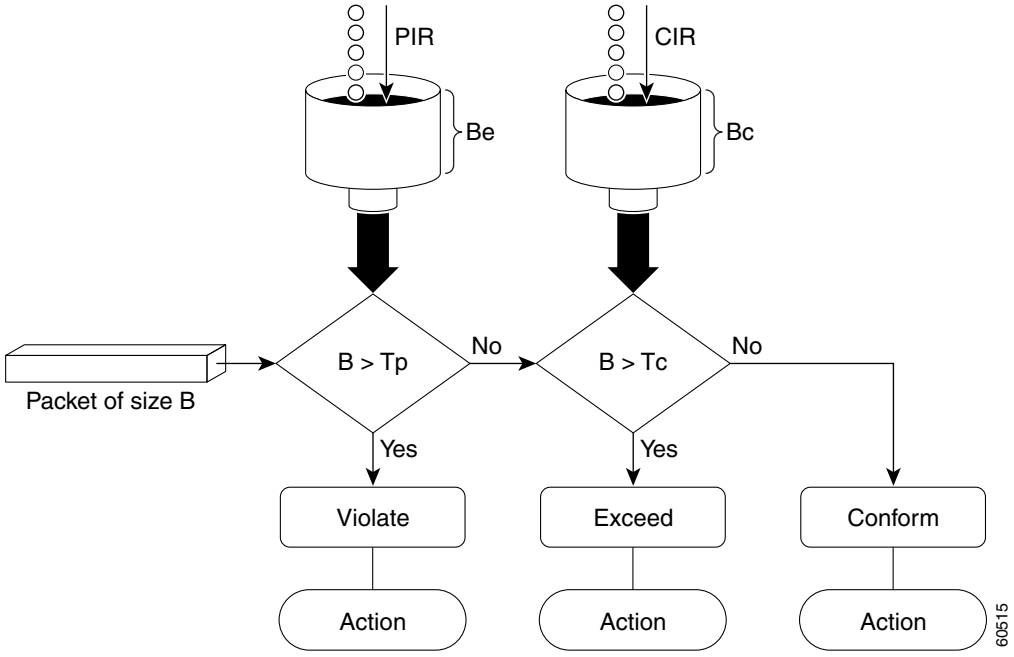
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate.
- 100 kbps would be marked as exceeding the rate.
- 50 kbps would be marked as violating the rate.

### Marking Packets and Assigning Actions Flowchart

The flowchart in Figure 2-1 illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

*Figure 2-1 Marking Packets and Assigning Actions with the Two-Rate Policer*




## Examples

This example shows how to configure two-rate traffic policing on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map police
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch# show policy-map policy1

 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Switch#
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

In the following example, 1.25 Mbps of traffic is sent (“offered”) to a policer class:

```
Switch# show policy-map interface gigabitethernet 6/1

 GigabitEthernet6/1

  Service-policy output: policy1

   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps

   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
Switch#
```

The two-rate policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming to the rate will be sent as is, and packets marked as exceeding the rate will be marked with IP Precedence 2 and then sent. Packets marked as violating the rate are dropped.

# policy-map

To create or modify a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode, use the **policy-map** global configuration command. To delete an existing policy map and to return to global configuration mode, use the **no** form of this command.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

## Syntax Description

| | |
|---|---|
| *policy-map-name* | Name of the policy map. |

## Defaults

No policy maps are defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(40)SG | Added support for the Supervisor Engine 6-E and Catalyst 4900M chassis. |

## Usage Guidelines

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created or modified. After you enter the **policy-map** command, the switch enters policy-map configuration mode. You can configure or modify the class policies for that policy map and decide how to treat the classified traffic.

These configuration commands are available in policy-map configuration mode:

- **class**: defines the classification match criteria for the specified class map. For more information, see the "class" section on page 2-50.
- **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.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

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.

## Examples

This example shows how to create a policy map called *policy1*. When attached to the ingress direction, it matches all the inbound 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. This policer action is applicable on all Catalyst 4500 Supervisors except the Supervisor Engine 6-E and Catalyst 4900M chassis.

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch#
```

This example shows how to configure multiple classes in a policy map called "policymap2" on a Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)# policy-map policymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 100000 20000 exceed-action
Switch(config-pmap-c)# set-dscp-transmit cs3
Switch(config-pmap-c)# set-cos-transmit 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police cir 32000 pir 64000 conform-action transmit exceed-action
Switch(config-pmap-c)# set-dscp-transmit cs3 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# exit
Switch#
```

This example shows how to delete the policy map called "policymap2":

```
Switch# configure terminal
Switch(config)# no policy-map policymap2
Switch#
```

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

## Related Commands

| Command | Description |
|---|---|
| **class** | Specifies the name of the class whose traffic policy you want to create or change. |
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **service-policy (interface configuration)** | Attaches a policy map to an interface or applies different QoS policies on VLANs that an interface belongs to. |
| **show policy-map** | Displays information about the policy map. |

# port-channel load-balance

To set the load-distribution method among the ports in the bundle, use the **port-channel load-balance** command. To reset the load distribution to the default, use the **no** form of this command.

**port-channel load-balance** *method*

**no port-channel load-balance**

## Syntax Description

| | |
|---|---|
| *method* | Specifies the load distribution method. See the "Usage Guidelines" section for more information. |

## Defaults

Load distribution on the source XOR destination IP address is enabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The following values are valid for the load-distribution method:

- **dst-ip**—Load distribution on the destination IP address
- **dst-mac**—Load distribution on the destination MAC address
- **dst-port**—Load distribution on the destination TCP/UDP port
- **src-dst-ip**—Load distribution on the source XOR destination IP address
- **src-dst-mac**—Load distribution on the source XOR destination MAC address
- **src-dst-port**—Load distribution on the source XOR destination TCP/UDP port
- **src-ip**—Load distribution on the source IP address
- **src-mac**—Load distribution on the source MAC address
- **src-port**—Load distribution on the source port

## Examples

This example shows how to set the load-distribution method to the destination IP address:

```
Switch(config)# port-channel load-balance dst-ip
Switch(config)#
```

This example shows how to set the load-distribution method to the source XOR destination IP address:

```
Switch(config)# port-channel load-balance src-dst-port
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| interface port-channel | Accesses or creates a port-channel interface. |
| show etherchannel | Displays EtherChannel information for a channel. |

# power dc input

To configure the power DC input parameters on the switch, use the **power dc input** command. To return to the default power settings, use the **no** form of this command.

**power dc input** *watts*

**no power dc input**

## Syntax Description

| | |
|---|---|
| **dc input** | Specifies the external DC source for both power supply slots. |
| *watts* | Sets the total capacity of the external DC source in watts; valid values are from 300 to 8500. |

## Defaults

DC power input is 2500 W.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(11)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(13)EW | Support for **dc input** was added. |

## Usage Guidelines

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface Admin
```

## Examples

This example shows how to set the total capacity of the external DC power source to 5000 W:

```
Switch(config)# power dc input 5000
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show power** | Displays information about the power status. |

# power inline

To set the inline-power state for the inline-power-capable interfaces, use the **power inline** command. To return to the default values, use the **no** form of this command.

**power inline** {**auto** [**max** *milliwatt*] | **never** | **static** [**max** *milliwatt*] | **consumption** *milliwatt*}

**no power inline**

## Syntax Description

| | |
|---|---|
| **auto** | Sets the Power over Ethernet state to auto mode for inline-power-capable interfaces. |
| **max** *milliwatt* | (Optional) Sets the maximum power that the equipment can consume; valid range is from 2000 to 15400 mW for classic modules. For the WS-X4648-RJ45V-E, the maximum is 20000. For the WS-X4648-RJ45V+E, the maximum is 30000. |
| **never** | Disables both the detection and power for the inline-power capable interfaces. |
| **static** | Allocates power statically. |
| **consumption** *milliwatt* | Sets power allocation per interface; valid range is from 4000 to 15400 for classic modules. Any non-default value disables automatic adjustment of power allocation. |

## Defaults

The default settings are as follows:

- Auto mode for Power over Ethernet is set.
- Maximum mW mode is set to 15400. For the WS-X4648-RJ45V-E, the maximum mW is set to 20000. For the WS-X4648-RJ45V+E, the maximum mW is set to 30000.
- Default allocation is set to 15400.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(11)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(19)EW | Support added for static power allocation. |
| 12.1(20)EW | Support added for Power over Ethernet. |
| 12.2(44)SG | Maximum supported wattage increased beyond 15400 for the WS-X4648-RJ45V-E and the WS-X4648-RJ45V+E. |

## Usage Guidelines

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface Admin
```

## Examples

This example shows how to set the inline-power detection and power for the inline-power-capable interfaces:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline auto
Switch(config-if)# end
Switch#
```

This example shows how to disable the inline-power detection and power for the inline-power-capable interfaces:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline never
Switch(config-if)# end
Switch#
```

This example shows how to set the permanent Power over Ethernet allocation to 8000 mW for Fast Ethernet interface 4/1 regardless what is mandated either by the 802.3af class of the discovered device or by any CDP packet that is received from the powered device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline consumption 8000
Switch(config-if)# end
Switch#
```

This example shows how to pre-allocate Power over Ethernet to 16500 mW for Gigabit Ethernet interface 2/1 regardless of what is mandated either by the 802.3af class of the discovered device or by any CDP packet that is received from the powered device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# power inline static max 16500
Switch(config-if)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| show power | Displays information about the power status. |

# power inline consumption

To set the default power that is allocated to an interface for all the inline-power-capable interfaces on the switch, use the **power inline consumption** command. To return to the default values, use the **no** form of this command.

**power inline consumption default** *milliwatts*

**no power inline consumption default**

## Syntax Description

| | |
|---|---|
| **default** | Specifies the switch to use the default allocation. |
| *milliwatts* | Sets the default power allocation in milliwatts; the valid range is from 4000 to 15400. Any non-default value disables automatic adjustment of power allocation. |

## Defaults

Milliwatt mode is set to 15400.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(11)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(20)EW | Support added for Power over Ethernet. |

## Usage Guidelines

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface Admin
```

## Examples

This example shows how to set the Power over Ethernet allocation to use 8000 mW, regardless of any CDP packet that is received from the powered device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power inline consumption default 8000
Switch(config)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| power inline | Sets the inline-power state for the inline-power-capable interfaces. |
| show power | Displays information about the power status. |

# power redundancy-mode

To configure the power settings for the chassis, use the **power redundancy-mode** command. To return to the default setting, use the **default** form of this command.

**power redundancy-mode** {**redundant** | **combined**}

**default power redundancy-mode**

## Syntax Description

| | |
|---|---|
| **redundant** | Configures the switch to redundant power management mode. |
| **combined** | Configures the switch to combined power management mode. |

## Defaults

Redundant power management mode

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. (Catalyst 4500 series switches only: 4503, 4506, and 4507). |

## Usage Guidelines

The two power supplies must be the same type and wattage.

**Caution** If you have power supplies with different types or wattages installed in your switch, the switch will not recognize one of the power supplies. A switch set to redundant mode will not have power redundancy. A switch set to combined mode will use only one power supply.

In redundant mode, the power from a single power supply must provide enough power to support the switch configuration.

Table 2-9 lists the maximum available power for chassis and Power over Ethernet for each power supply.

*Table 2-9 Available Power*

| Power Supply | Redundant Mode (W) | Combined Mode (W) |
|---|---|---|
| 1000 W AC | System[1] = 1000 | System = 1667 |
| | Inline = 0 | Inline = 0 |
| 2800 W AC | System = 1360 | System = 2473 |
| | Inline = 1400 | Inline = 2333 |

1. The system power includes power for the supervisor engines, all modules, and the fan tray.

## Examples

This example shows how to set the power management mode to combined:

```
Switch(config)# power redundancy-mode combined
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| show power | Displays information about the power status. |

# port-security mac-address

To configure a secure address on an interface for a specific VLAN or VLAN range, use the **port-security mac-address** command.

**port-security mac-address** *mac_address*

## Syntax Description

| | |
|---|---|
| *mac_address* | The MAC-address that needs to be secured. |

## Command Modes

VLAN-range interface submode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EWA | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the **vlan** command, you can use the **port-security mac-address** command to specify different addresses on different VLANs.

## Examples

This example shows how to configure the secure address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **port-security mac-address sticky** | Configures a sticky address on an interface for a specific VLAN or VLAN range. |
| **port-security maximum** | Configures the maximum number of addresses on an interface for a specific VLAN or VLAN range. |

# port-security mac-address sticky

To configure a sticky address on an interface for a specific VLAN or VLAN range, use the **port-security mac-address sticky** command.

**port-security mac-address sticky** *mac_address*

## Syntax Description

| | |
|---|---|
| *mac_address* | The MAC-address that needs to be secured. |

## Command Modes

VLAN-range interface submode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EWA | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The Sticky feature must be enabled on an interface before you can configure the **port-security mac-address sticky** command.

## Usage Guidelines

Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the **vlan** command, you can use the **port-security mac-address sticky** command to specify different sticky addresses on different VLANs.

The Sticky feature must be enabled on an interface before you can configure the **port-security mac-address sticky** command.

Sticky MAC addresses are addresses that persist across switch reboots and link flaps.

## Examples

This example shows how to configure the sticky address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.1
Switch(config-if-vlan-range)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| port-security mac-address | Configures a secure address on an interface for a specific VLAN or VLAN range. |
| port-security maximum | Configures the maximum number of addresses on an interface for a specific VLAN or VLAN range. |

# port-security maximum

To configure the maximum number of addresses on an interface for a specific VLAN or VLAN range, use the **port-security maximum** command.

**port-security maximum** *max_value*

## Syntax Description

| | |
|---|---|
| *max_value* | The maximum number of MAC-addresses. |

## Command Modes

VLAN-range interface submode

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EWA | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the **vlan** command, you can use the **port-security maximum** command to specify the maximum number of secure addresses on different VLANs.

If a specific VLAN on a port is not configured with a maximum value, the maximum configured for the port is used for that VLAN. In this situation, the maximum number of addresses that can be secured on this VLAN is limited to the maximum value configured on the port.

Each VLAN can be configured with a maximum count that is greater than the value configured on the port. Also, the sum total of the maximum configured values for all the VLANs can exceed the maximum configured for the port. In either of these situations, the number of MAC addresses secured on each VLAN is limited to the lesser of the VLAN configuration maximum and the port configuration maximum.

## Examples

This example shows how to configure a maximum number of addresses (5) on interface Gigabit Ethernet 1/1 for VLANs 2-3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security maximum 5
Switch(config-if-vlan-range)# exit
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| port-security mac-address | Configures a secure address on an interface for a specific VLAN or VLAN range. |
| port-security mac-address sticky | Configures a sticky address on an interface for a specific VLAN or VLAN range. |

# power inline police

To configure PoE policing on a particular interface, use the **power inline police** command. The **no** form of the command disables PoE policing on an interface.

**power inline police** [**action**] [**errdisable | log**]

[**no**] **power inline police** [**action**] [**errdisable | log**]

## Syntax Description

| | |
|---|---|
| **action** | (optional) Specifies the action to take on the port when a PoE policing fault occurs (the device consumes more power than it's allocated). |
| **errdisable** | (optional) Enables PoE policing on the interface and places the port in an errdisable state when a PoE policing fault occurs. |
| **log** | (optional) Enables PoE policing on the interface and, if a PoE policing fault occurs, shuts, restarts the port, and logs an error message. |

## Defaults

PoE policing is disabled.

## Command Modes

Interface Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If a port is in the errdisable state because of a PoE policing fault, enter the **shut** command followed by a **no shut** on the interface to make the port operational again.

You can also configure inline-power errdisable autorecovery so that an errdisabled interface is automatically revived when the errdisable autorecovery timer expires.

## Examples

This example shows how to enable PoE policing and configure a policing action:

```
Switch(config)# int gigabitEthernet 2/1
Switch(config-if)# power inline police
Switch(config-if)# do show power inline police gigabitEthernet 2/1
Available:421(w)  Used:39(w)  Remaining:382(w)

Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi2/1     auto   on         errdisable ok         17.4   7.6


Switch(config-if)# power inline police action log
Available:421(w)  Used:39(w)  Remaining:382(w)
```

```
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi2/1     auto   on         log        ok         17.4   9.6
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show power inline police** | Displays the PoE policing status of an interface, module, or chassis. |
| **errdisable recovery cause inline-power** (refer to Cisco IOS documentation) | Enables errdisable autorecovery; the port automatically restarts itself after going to the errdisable state after its errdisable autorecovery timer expires. |

# pppoe intermediate-agent (global)

To enable the PPPoE Intermediate Agent feature on a switch, use the **pppoe intermediate-agent** global configuration command. To disable the feature, use the **no** form of this command.

**pppoe intermediate-agent**

[**no**] **pppoe intermediate-agent**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

You must enable PPPoE Intermediate Agent globally on a switch before you can use PPPoE Intermediate Agent on an interface or interface VLAN.

## Examples

This example shows how to enable PPPoE Intermediate Agent on a switch:

```
Switch(config)# pppoe intermediate-agent
Switch(config)#
```

This example shows how to disable PPPoE Intermediate Agent on a switch:

```
Switch(config)# no pppoe intermediate-agent
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| pppoe intermediate-agent format-type (global) | Sets the access node identifier, generic error message, and identifier string for a switch. |

# pppoe intermediate-agent (interface)

**Note** This command takes effect only if you enable the **pppoe intermediate-agent** global command.

To enable the PPPoE Intermediate Agent feature on an interface, use the **pppoe intermediate-agent** command. To disable the feature, use the **no** form of this command.

**pppoe intermediate-agent**

[**no**] **pppoe intermediate-agent**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled on all interfaces.

## Command Modes

Interface Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

PPPoE Intermediate Agent is enabled on an interface provided the PPPoE Intermediate Agent is enabled both on the switch and the interface.

## Examples

This example shows how to enable the PPPoE Intermediate Agent on an interface:

```
Switch(config-if)# pppoe intermediate-agent
Switch(config-if)#
```

This example shows how to disable the PPPoE Intermediate Agent on an interface:

```
Switch(config-if)# no pppoe intermediate-agent
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| pppoe intermediate-agent format-type (global) | Sets circuit ID or remote ID for an interface. |
| pppoe intermediate-agent limit rate | Limits the rate of the PPPoE Discovery packets coming on an interface. |

| Command | Description |
|---|---|
| **pppoe intermediate-agent trust** | Sets the trust configuration of an interface. |
| **pppoe intermediate-agent vendor-tag strip** | Enables vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS). |

# pppoe intermediate-agent (interface vlan-range)

**Note** This command takes effect only if you enable the **pppoe intermediate-agent** global command.

To enable PPPoE Intermediate Agent on an interface VLAN range, use the **pppoe intermediate-agent** global command. To disable the feature, use the **no** form of this command.

**pppoe intermediate-agent**

[**no**] **pppoe intermediate-agent**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled on all VLANs on all interfaces.

## Command Modes

Interface Vlan-Range Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Although this command takes effect irrespective of the **pppoe intermediate-agent** (interface configuration mode) command, you must enable the **pppoe intermediate-agent** (global configuration mode) command.

## Examples

This example shows how to enable PPPoE Intermediate Agent on a range of VLANs:

```
Switch(config-if)# vlan-range 167-368
Switch(config-if-vlan-range)# pppoe intermediate-agent
Switch(config-if-vlan-range)#
```

This example shows how to disable PPPoE Intermediate Agent on a single VLAN:

```
Switch(config-if)# vlan-range 268
Switch(config-if-vlan-range)# no pppoe intermediate-agent
Switch(config-if-vlan-range)#
```

## Related Commands

| Command | Description |
|---|---|
| pppoe intermediate-agent (interface) | Enables the PPPoE Intermediate Agent feature on an interface. |

# pppoe intermediate-agent format-type (global)

To set the access node identifier, generic error message, and identifier string for the switch, use the **pppoe intermediate-agent format-type (global)** command. To disable the feature, use the **no** form of this command

**pppoe intermediate-agent format-type access-node-identifier string** *string*

**pppoe intermediate-agent format-type generic-error-message string** *string*

**pppoe intermediate-agent format-type identifier-string string** *string* **option {sp | sv | pv | spv} delimiter {**, | . | ; | / | #**}**

**no pppoe intermediate-agent format-type** {**access-node-identifier | generic-error-message | identifier-string**}

## Syntax Description

| | |
|---|---|
| **access-node-identifier string** *string* | ASCII string literal value for the access-node-identifier |
| **generic-error-message string** *string* | ASCII string literal value for the generic-error-message |
| **identifier-string string** *string* | ASCII string literal value for the identifier-string |
| **option** {**sp** \| **sv** \| **pv** \| **spv**} | Options:<br>**sp** = slot + port<br>**sv** = slot + vlan<br>**pv** = port + vlan<br>**spv** = slot + port + vlan |
| delimiter {, \| . \| ; \| / \| #} | Delimiter between slot/port/vlan portions of **option** |

## Defaults

**access-node-identifier** has a default value of 0.0.0.0.

**generic-error-message**, **identifier-string**, **option**, and **delimiter** have no default values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Use the **access-node-identifier** and **identifier-string** commands to enable the switch to generate the circuit-id parameters automatically.

The **no** form of **identifier-string** command unsets the option and delimiter.

Use the **generic-error-message** command to set an error message notifying the sender that the PPPoE Discovery packet was too large.

## Examples

This example shows how to set an access-node-identifier:

```
Switch(config)# pppoe intermediate-agent format-type access-node-identifier string
switch-abc-123
Switch(config)#
```

This example shows how to unset a generic-error-message:

```
Switch(config)# no pppoe intermediate-agent format-type generic-error-message
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show pppoe intermediate-agent information** (refer to Cisco IOS documentation) | Displays the PPPoE Intermediate Agent configuration and statistics (packet counters). |

# pppoe intermediate-agent format-type (interface)

**Note** This command takes effect only if you enable the **pppoe intermediate-agent** interface configuration command.

To set circuit-id or remote-id for an interface, use the **pppoe intermediate-agent format-type** command. To unset the parameters, use the **no** form of this command.

**pppoe intermediate-agent format-type** {**circuit-id** | **remote-id**} **string** *string*

[**no**] **pppoe intermediate-agent format-type** {**circuit-id** | **remote-id**} **string** *string*

## Syntax Description

| | |
|---|---|
| **circuit-id string** *string* | ASCII string literal value for circuit-id |
| **remote-id string** *string* | ASCII string literal value for remote-id |

## Defaults

No default values for circuit-id and remote-id.

## Command Modes

Interface Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Use the **pppoe intermediate-agent format-type** command to set interface-specific circuit-id and remote-id values. If interface-specific circuit-id is not set, the system's automatic generated circuit-id value is used.

## Examples

This example shows how to set remote-id for an interface:

```
Switch(config-if)# pppoe intermediate-agent format-type remote-id string user5551983
Switch(config-if)#
```

This example shows how to unset circuit-id for an interface:

```
Switch(config)# no pppoe intermediate-agent format-type circuit-id
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| pppoe intermediate-agent (interface) | Enables the PPPoE Intermediate Agent feature on an interface. |
| pppoe intermediate-agent (interface vlan-range) | Sets the circuit-id or remote-id for an interface vlan-range. |

# pppoe intermediate-agent format-type (interface vlan-range)

**Note** This command takes effect only if you enable the **pppoe intermediate-agent** interface vlan-range configuration mode command.

To set circuit-id or remote-id for an interface vlan-range, use the **pppoe intermediate-agent format-type** interface vlan-range mode command. To unset the parameters, use the **no** form of this command.

**pppoe intermediate-agent format-type** {**circuit-id** | **remote-id**} **string** *string*

[**no**] **pppoe intermediate-agent format-type** {**circuit-id** | **remote-id**} **string** *string*

## Syntax Description

| | |
|---|---|
| **circuit-id string** *string* | ASCII string literal value to be set for circuit-id |
| **remote-id string** *string* | ASCII string literal value to be set for remote-id |

## Defaults

No default values for circuit-id and remote-id.

## Command Modes

Interface Vlan-Range Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Use these commands to set circuit-id or remote-id on an interface vlan-range. If circuit-id is not set, the system's automatically generated circuit-id is used.

## Examples

This example shows how to set remote-id on an interface VLAN:

```
Switch(config-if)# vlan-range 268
Switch(config-if-vlan-range)# pppoe intermediate-agent format-type remote-id string user5551983-cabletv
Switch(config-if-vlan-range)#
```

This example shows how to unset circuit-id on an interface vlan-range:

```
Switch(config-if)# vlan-range 167-368
Switch(config-if-vlan-range)# no pppoe intermediate-agent format-type circuit-id
Switch(config-if-vlan-range)#
```

## Related Commands

| Command | Description |
|---|---|
| **pppoe intermediate-agent (interface vlan-range)** | Enables PPPoE Intermediate Agent on an interface VLAN range. |

# pppoe intermediate-agent limit rate

To limit the rate of the PPPoE Discovery packets arriving on an interface, use the **pppoe intermediate-agent limit rate** command. To disable the feature, use the **no** form of this command.

**pppoe intermediate-agent limit rate** *number*

[**no**] **pppoe intermediate-agent limit rate** *number*

## Syntax Description

| | |
|---|---|
| **rate** *number* | Specifies the threshold rate of PPPoE Discovery packets received on this interface in *packets-per-second*. |

## Defaults

This command has no default settings.

## Command Modes

Interface Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If this command is used and PPPoE Discovery packets received exceeds the rate set, the interface will be error-disabled (shutdown).

## Examples

This example shows how to set a rate limit for an interface:

```
Switch(config-if)# pppoe intermediate-agent limit rate 50
Switch(config-if)#
```

This example shows how to disable rate limiting for an interface:

```
Switch(config-if)# no pppoe intermediate-agent limit rate
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| pppoe intermediate-agent (interface) | Enables the PPPoE Intermediate Agent feature on an interface |

# pppoe intermediate-agent trust

To set the trust configuration of an interface, use the **pppoe intermediate-agent trust** global command. To unset the trust parameter, use the **no** form of this command.

[**no**] **pppoe intermediate-agent trust**

[**no**] **pppoe intermediate-agent trust**

## Syntax Description

This command has no arguments or keywords.

## Defaults

All interfaces are untrusted.

## Command Modes

Interface Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

At least one trusted interface must be present on the switch for PPPoE Intermediate Agent feature to work.

Set the interface connecting the switch to the PPPoE Server (or BRAS) as trusted.

## Examples

This example shows how to set an interface as trusted:

```
Switch(config-if)# pppoe intermediate-agent trust
Switch(config-if)#
```

This example shows how to disable the trust configuration for an interface:

```
Switch(config-if)# no pppoe intermediate-agent trust
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| pppoe intermediate-agent vendor-tag strip | Enables vendor-tag stripping on PPPoE Discovery packets from a PPPoE Server (or BRAS). |

# pppoe intermediate-agent vendor-tag strip

**Note** This command takes effect only if you enable the **pppoe intermediate-agent** interface configuration command and the **pppoe intermediate-agent trust** command.

To enable vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS), use the **pppoe intermediate-agent vendor-tag strip** command. To disable this setting, use the **no** form of this command.

**pppoe intermediate-agent vendor-tag strip**

[**no**] **pppoe intermediate-agent vendor-tag strip**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Vendor-tag stripping is turned off.

## Command Modes

Interface Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command has no effect on untrusted interfaces.

Use this command on a PPPoE Intermediate Agent trusted interface to strip off the vendor-specific tags in PPPoE Discovery packets that arrive downstream from the PPPoE Server (or BRAS), if any.

## Examples

This example shows how to set vendor-tag stripping on an interface:

```
Switch(config-if)# pppoe intermediate-agent vendor-tag strip
Switch(config-if)#
```

This example shows how to disable vendor-tag stripping on an interface:

```
Switch(config-if)# no pppoe intermediate-agent vendor-tag strip
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| pppoe intermediate-agent (interface) | Enables the PPPoE Intermediate Agent feature on an interface. |
| pppoe intermediate-agent trust | Sets the trust configuration of an interface. |

# priority

To enable the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port, use the **priority** policy-map class configuration command. To return to the default setting, use the **no** form of this command.

**priority**

**no priority**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The strict priority queue is disabled.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E. |

## Usage Guidelines

Use the **priority** command only in a policy map attached to a physical port. You can use this command only in class-level classes, you cannot use this command in class class-default.

This command configures LLQ and provides strict-priority queueing. Strict-priority queueing enables delay-sensitive data, such as voice, to be sent before packets in other queues are sent. The priority queue is serviced first until it is empty.

You cannot use the **bandwidth**, **dbl**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

You can use police or set class configuration commands with the priority police-map class configuration command.

If the priority queuing class is not rate limited, you cannot use the bandwidth command, you can use the bandwidth remaining percent command instead.

## Examples

This example shows how to enable the LLQ for the policy map called *policy1*:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
```

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

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port. |
| **class** | Specifies the name of the class whose traffic policy you want to create or change. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **dbl** | Enables dynamic buffer limiting for traffic hitting this class. |
| **service-policy (policy-map class)** | Creates a service policy that is a quality of service (QoS) policy within a policy map. |
| **shape (class-based queueing)** | Enables traffic shaping a class of traffic in a policy map attached to a physical port. |
| **show policy-map** | Displays information about the policy map. |

# private-vlan

To configure private VLANs and the association between a private VLAN and a secondary VLAN, use the **private-vlan** command. To return to the default value, use the **no** form of this command.

**private-vlan** {**isolated** | **community** | **primary**}

**private-vlan association** *secondary-vlan-list* [{**add** *secondary-vlan-list*} | {**remove** *secondary-vlan-list*}]

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

**no private-vlan association**

## Syntax Description

| | |
|---|---|
| **isolated** | Designates the VLAN as an isolated private VLAN. |
| **community** | Designates the VLAN as the community private VLAN. |
| **primary** | Designates the VLAN as the primary private VLAN. |
| **association** | Creates an association between a secondary VLAN and a primary VLAN. |
| *secondary-vlan-list* | Specifies the number of the secondary VLAN. |
| **add** | (Optional) Associates a secondary VLAN to a primary VLAN. |
| **remove** | (Optional) Clears the association between a secondary VLAN and a primary VLAN. |

## Defaults

Private VLANs are not configured.

## Command Modes

VLAN configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(12c)EW | Support for extended addressing was added. |
| 12.2(20)EW | Support for community VLAN was added. |

## Usage Guidelines

You cannot configure VLAN 1 or VLANs 1001 to 1005 as private VLANs.

VTP does not support private VLANs. You must configure private VLANs on each device where you want private VLAN ports.

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 range of private VLAN IDs separated by hyphens.

The *secondary_vlan_list* parameter can contain multiple community VLAN IDs.

The *secondary_vlan_list* parameter can contain only one isolated VLAN ID. A private VLAN is defined as a set of private ports characterized by a common set of VLAN number pairs: each pair is made up of at least two special unidirectional VLANs and is used by isolated ports or by a community of ports to communicate with the switches.

An isolated VLAN is a VLAN that is used by the isolated ports to communicate with the promiscuous ports. The isolated VLAN traffic is blocked on all other private ports in the same VLAN and can be received only by the standard trunking ports and the promiscuous ports that are assigned to the corresponding primary VLAN.

A community VLAN is the VLAN that carries the traffic among the community ports and from the community ports to the promiscuous ports on the corresponding primary VLAN. A community VLAN is not allowed on a private VLAN trunk.

A promiscuous port is a private port that is assigned to a primary VLAN.

A primary VLAN is a VLAN that is used to convey the traffic from the switches to the customer end stations on the private ports.

You can specify only one isolated *vlan-id* value, while multiple community VLANs are allowed. You can only associate isolated and community VLANs to one VLAN. The associated VLAN list may not contain primary VLANs. Similarly, a VLAN that is already associated to a primary VLAN cannot be configured as a primary VLAN.

The **private-vlan** commands do not take effect until you exit the config-VLAN submode.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.

Refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional configuration guidelines.

## Examples

This example shows how to configure VLAN 202 as a primary VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# end
Switch# show vlan private-vlan
Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
```

This example shows how to configure VLAN 303 as a community VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 303
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
```

This example shows how to configure VLAN 440 as an isolated VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 440
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# end
```

```
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
        440       isolated
```

This example shows how to create a private VLAN relationship among the primary VLAN 14, the isolated VLAN 19, and community VLANs 20 and 21:

```
Switch(config)# vlan 19
Switch(config-vlan) # private-vlan isolated
Switch(config)# vlan 14
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 19
```

This example shows how to remove a private VLAN relationship and delete the primary VLAN. The associated secondary VLANs are not deleted.

```
Switch(config-vlan)# no private-vlan 14
Switch(config-vlan)#
```

This example shows how to associate community VLANs 303 through 307 and 309 and isolated VLAN 440 with primary VLAN 202 and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 303-307,309,440
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
        308       community
```

**Note** The secondary VLAN 308 has no associated primary VLAN.

This example shows how to remove an isolated VLAN from the private VLAN association:

```
Switch(config)# vlan 14
Switch(config-vlan)# private-vlan association remove 18
Switch(config-vlan)#
```

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end

Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
```

```
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation : dot1q
  Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays VLAN information. |
| **show vlan private-vlan** | Displays private VLAN information. |

# private-vlan mapping

To create a mapping between the primary and the secondary VLANs so that both share the same primary VLAN SVI, use the **private-vlan mapping** command. To remove all PVLAN mappings from an SVI, use the **no** form of this command.

**private-vlan mapping** *primary-vlan-id* {[*secondary-vlan-list* | {**add** *secondary-vlan-list*} | {**remove** *secondary-vlan-list*}]}

**no private-vlan mapping**

## Syntax Description

| | |
|---|---|
| *primary-vlan-id* | VLAN ID of the primary VLAN of the PVLAN relationship. |
| *secondary-vlan-list* | (Optional) VLAN ID of the secondary VLANs to map to the primary VLAN. |
| **add** | (Optional) Maps the secondary VLAN to the primary VLAN. |
| **remove** | (Optional) Removes the mapping between the secondary VLAN and the primary VLAN. |

## Defaults

All PVLAN mappings are removed.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple, comma-separated items. Each item can be a single PVLAN ID or a range of PVLAN IDs separated by hyphens.

This command is valid in the interface configuration mode of the primary VLAN.

The SVI of the primary VLAN is created at Layer 3.

The traffic that is received on the secondary VLAN is routed by the SVI of the primary VLAN.

The SVIs of the existing secondary VLANs do not function and are considered down after this command is entered.

A secondary SVI can be mapped to only one primary SVI. If the configured PVLANs association is different from what is specified in this command (if the specified *primary-vlan-id* is configured as a secondary VLAN), all the SVIs that are specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 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(config)# interface vlan 18
Switch(config-if)# private-vlan mapping 18 20
Switch(config-if)#
```

This example shows how to permit the routing of the secondary VLAN ingress traffic from PVLANs 303 through 307, 309, and 440 and how to verify the configuration:

```
Switch# config terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            isolated
vlan202   304            isolated
vlan202   305            isolated
vlan202   306            isolated
vlan202   307            isolated
vlan202   309            isolated
vlan202   440            isolated
Switch#
```

This example shows the displayed message that you will see if the VLAN that you are adding is already mapped to the SVI of VLAN 18. You must delete the mapping from the SVI of VLAN 18 first.

```
Switch(config)# interface vlan 19
Switch(config-if)# private-vlan mapping 19 add 21
    Command rejected: The interface for VLAN 21 is already mapped as s secondary.
Switch(config-if)#
```

This example shows how to remove all PVLAN mappings from the SVI of VLAN 19:

```
Switch(config)# interface vlan 19
Switch(config-if)# no private-vlan mapping
Switch(config-if)#


Switch# configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            community
vlan202   304            community
vlan202   305            community
vlan202   306            community
vlan202   307            community
vlan202   309            community
vlan202   440            isolated

Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces private-vlan mapping** | Displays PVLAN mapping information for VLAN SVIs. |
| **show vlan** | Displays VLAN information. |
| **show vlan private-vlan** | Displays private VLAN information. |

# private-vlan synchronize

To map the secondary VLANs to the same instance as the primary VLAN, use the **private-vlan synchronize** command.

**private-vlan synchronize**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

MST configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If you do not map the VLANs to the same instance as the associated primary VLAN when you exit the MST configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

## Examples

This example shows how to initialize PVLAN synchronization:

```
Switch(config-mst)# private-vlan synchronize
Switch(config-mst)#
```

This example assumes that a primary VLAN 2 and a secondary VLAN 3 are associated to VLAN 2, and that all VLANs are mapped to the CIST instance 1. This example also shows the output if you try to change the mapping for the primary VLAN 2 only:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 2
Switch(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
->3
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| show spanning-tree mst | Displays MST protocol information. |

# qos (global configuration mode)

To globally enable QoS functionality on the switch, use the **qos** command. To globally disable QoS functionality, use the **no** form of this command.

**qos**

**no qos**

## Syntax Description

This command has no arguments or keywords.

## Defaults

QoS functionality is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. On the Supervisor Engine 6-E and Catalyst 4900M chassis QoS is always enabled without being configured.

If QoS functionality is globally enabled, it is enabled on all interfaces, except on the interfaces where QoS has been disabled. If QoS functionality is globally disabled, all traffic is passed in QoS pass-through mode.

## Examples

This example shows how to enable QoS functionality globally on the switch:

```
Switch(config)# qos
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| qos (interface configuration mode) | Enables QoS functionality on an interface. |
| show qos | Displays QoS information. |

# qos (interface configuration mode)

To enable QoS functionality on an interface, use the **qos** command. To disable QoS functionality on an interface, use the **no** form of this command.

**qos**

**no qos**

## Syntax Description

This command has no arguments or keywords.

## Defaults

QoS is enabled.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. On the Supervisor Engine 6-E and Catlyst 4900M chassis, attaching a service policy implicitly enables QoS on the supervisor engine and detaching a service policy implicitly disables QoS on the supervisor engine.

If QoS functionality is globally disabled, it is also disabled on all interfaces.

## Examples

This example shows how to enable QoS functionality on an interface:

```
Switch(config-if)# qos
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| qos (global configuration mode) | Enables QoS functionality on the switch. |
| qos (interface configuration mode) | Enables QoS functionality on an interface. |
| show qos | Displays QoS information. |

# qos account layer2 encapsulation

To include additional bytes to be accounted by the QoS features, use the **qos account layer2 encapsulation** command. To disable the use of additional bytes, use the **no** form of this command.

**qos account layer2 encapsulation** {**arpa** | **dot1q** | **isl** | **length** *len*}

**no qos account layer2 encapsulation** {**arpa** | **dot1q** | **isl** | **length** *len*}

## Syntax Description

| | |
|---|---|
| **arpa** | Specifies the account length of the Ethernet ARPA-encapsulated packet (18 bytes). |
| **dot1q** | Specifies the account length of the 802.1Q-encapsulated packet (22 bytes). |
| **isl** | Specifies the account length of the ISL-encapsulated packet (48 bytes). |
| **length** *len* | Specifies the a dditional packet length to account for; the valid range is from 0 to 64 bytes. |

## Defaults

On non-Supervisor Engine 6-Es only the length that is specified in the IP header for the IP packets and the length that is specified in the Ethernet header for non-IP packets are included.

On the Supervisor Engine 6-E and Catalyst 4900M chassis the length that is specified in the Ethernet header is taken into account for both IP and non-IP packets. The Layer 2 length includes the VLAN tag overhead too.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

In the Catalyst 4500 series switch, for non-Superviosr Engine 6-E supervisors the **qos account layer2 encapsulation** command indicates that the policing feature should consider the configured length in addition to the IP length of the packet when policing the IP packets.

Sharing and shaping always use the Ethernet ARPA length.

On Supervisor Engine 6-E and Catalyst 4900M chassis shaping and sharing always use Ethernet ARPA length to which 20 bytes of IPv6 overhead is always added for policing. However, only Layer 2 length, including VLAN tag overhead is taken into account.

**Note** The given length is included when policing all IP packets irrespective of the encapsulation with which it was received. When **qos account layer2 encapsulation isl** is configured, a fixed length of 48 bytes is included when policing all IP packets, not only those IP packets that are received with ISL encapsulation.

Sharing and shaping use the length that is specified in the Layer 2 headers.

## Examples

This example shows how to include an additional 18 bytes when policing IP packets:

```
Switch# config terminal
Switch(conf)# qos account layer2 encapsulation length 18
Switch (conf)# end
Switch#
```

This example shows how to disable the consistent accounting of the Layer 2 encapsulation by the QoS features:

```
Switch# config terminal
Switch(config)# no qos account layer2 encapsulation
Switch (config)# end
Switch #
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays traffic on a specific interface. |
| **switchport** | Modifies the switching characteristics of a Layer 2 switch interface. |
| **switchport block** | Prevents the unknown multicast or unicast packets from being forwarded. |

# qos aggregate-policer

To define a named aggregate policer, use the **qos aggregate-policer** command. To delete a named aggregate policer, use the **no** form of this command.

**qos aggregate-policer** *name rate burst* [**conform-action** {**transmit** | **drop**} | **exceed-action** {**transmit** | **drop** | **policed-dscp-transmit**}]

**no qos aggregate-policer** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the aggregate policer. |
| *rate* | Maximum bits per second; valid values are from 32000 to 32000000000. |
| *burst* | Burst bytes; valid values are from 1000 to 512000000. |
| **conform-action** | (Optional) Specifies the action to be taken when the rate is not exceeded. |
| **transmit** | (Optional) Transmits the package. |
| **drop** | (Optional) Drops the packet. |
| **exceed-action** | (Optional) Specifies action when the QoS values are exceeded. |
| **policed-dscp-transmit** | (Optional) Sends the DSCP per the policed-DSCP map. |

## Defaults

The default settings are as follows:

- Conform-action transmits
- Exceed-action drops

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

This policer can be shared by different policy map classes and on different interfaces.

The Catalyst 4506 switch supports up to 1000 aggregate input policers and 1000 output policers.

The **qos aggregate-policer** command allows you to configure an aggregate flow and a policing rule for that aggregate. When you enter your rate and burst parameters, the range for the average rate is 32 Kbps to 32 Gbps, and the range for the burst size is 1 KB to 512 MB.

A rate can be entered in bits-per-second without a suffix. In addition, the suffixes described in Table 2-10 are allowed.

*Table 2-10 Rate Suffix*

| Suffix | Description |
|---|---|
| k | 1000 bps |
| m | 1,000,000 bps |
| g | 1,000,000,000 bps |

Bursts can be entered in bytes without a suffix. In addition, the suffixes shown in Table 2-11 are allowed.

*Table 2-11 Burst Suffix*

| Suffix | Description |
|---|---|
| k | 1000 bytes |
| m | 1,000,000 bytes |
| g | 1,000,000,000 bytes |

**Note** Due to hardware granularity, the rate value is limited, so the burst that you configure might not be the value that is used.

Modifying an existing aggregate rate limit modifies that entry in NVRAM and in the switch if it is currently being used.

When you enter the aggregate policer name, follow these naming conventions:

- Maximum of 31 characters long and may include a-z, A-Z, 0-9, the dash (-), the underscore (_), and the period (.).
- Must start with an alphabetic character and must be unique across all ACLs of all types.
- Aggregate policer names are case sensitive.
- Cannot be a number.
- Must not be a keyword; keywords to avoid are **all**, **default-action**, **map**, **help**, and **editbuffer**.

An aggregate policer can be applied to one or more interfaces. However, if you apply the same policer to the input direction on one interface and to the output direction on a different interface, then you have created the equivalent of two different aggregate policers in the switching engine. Each policer has the same policing parameters, with one policing the ingress traffic on one interface and the other policing the egress traffic on another interface. If you apply an aggregate policer to multiple interfaces in the same direction, only one instance of the policer is created in the switching engine.

You can apply an aggregate policer to a physical interface or to a VLAN. If you apply the same aggregate policer to a physical interface and to a VLAN, then you have created the equivalent of two different aggregate policers in the switching engine. Each policer has the same policing parameters, with one policing the traffic on the configured physical interface and the other policing the traffic on the configured VLAN. If you apply an aggregate policer to only ports or only VLANs, then only one instance of the policer is created in the switching engine.

If you apply a single aggregate policer to the ports and the VLANs in different directions, then you have created the equivalent of four aggregate policers; one for all ports sharing the policer inthe input direction, one for all ports sharing the policer in the output direction, one for all VLANs sharing the policer in the input direction, and one for all VLANs sharing the policer in the output direction.

## Examples

This example shows how to configure a QoS aggregate policer to allow a maximum of 100,000 bits per second with a normal burst size of 10,000 bytes, to transmit when these rates are not exceeded, and to drop packets when these rates are exceeded:

```
Switch(config)# qos aggregate-policer micro-one 100000 10000 conform-action transmit exceed-action drop
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| show qos aggregate policer | Displays QoS aggregate policer information. |

# qos control-packets

To enable Layer 2 control packet QoS mode on control packets use the **qos control-packets** command. To disable Layer 2 control packet QoS mode on control packets, use the **no** form of this command.

**qos control-packets** {**bpdu-range** | **cdp-vtp** | **sstp** | **lldp**}

**no qos control-packets** {**bpdu-range** | **cdp-vtp** | **sstp** | **lldp**}

## Syntax Description

| | |
|---|---|
| **bpdu-range** | Specifies enabling QoS on BPDU-range packets. |
| **cdp-vtp** | Specifies enabling QoS on CDP and VTP packets. |
| **sstp** | Specifies enabling QoS on SSTP packets. |
| **lldp** | Specifies enabling QoS on LLDP packets. |

## Defaults

This command has no default settings.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(46)SG | Support for thre **lldp** keyword. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

The ranges of addresses that Layer 2 control packet QoS acts on when the relative command is entered is shown in Table 2-12:

*Table 2-12 Packet Type and Actionable Address Range*

| Type of Packet on Which Feature is Enabled | Range of address |
|---|---|
| BPDU-range | 0180.C200.0000 BPDU<br>0180.C200.0002 OAM, LACP<br>0180.C200.0003 Eapol |
| CDP-VTP | 0100.0CCC.CCCC |
| SSTP | 0100.0CCC.CCCD |
| LLDP | 0180.C200.000E |

**Note** If you enter **qos control-packet** without specifying any control packet types, the feature is enabled for all of them.

When Layer 2 control packet QoS is enabled, you need to configure policies to match the required Layer 2 packets and police them as desired. When the feature is enabled on a particular packet type, MACLs that match the desired control packets are automatically generated, if not already present. The corresponding class maps matching these MACLs are auto-generated as well. You can then use these class maps in the policy maps in order to police the control packets, applying them a per port, per VLAN, or per port per VLAN just like any other policy map. In addition, you can define your own MACLs/class maps to match the control packets. The only limitation is that the user-defined class maps have to begin with the prefix “system-control-packet-”.

## Examples

This example shows how to enable QoS on BDPU packets.

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets bpdu-range
Switch(config)#
```

This example shows how to enable QoS on CDP and VTP packets.

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets cdp-vtp
Switch(config)#
```

This example shows how to enable QoS on SSTP packets.

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets sstp
Switch(config)#
```

This example shows how to enable QoS on LLDP packets:

```
Switch# enable
Switch# configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# qos control-packets lldp
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| show policy-map interface | Displays the statistics and configurations of the input and output policies that are attached to an interface. |
| show running-config | Displays the running-configuration for a switch. |

# qos cos

To define the default CoS value for an interface, use the **qos cos** command. To remove a prior entry, use the **no** form of this command.

**qos cos** *cos_value*

**no qos cos** *cos_value*

## Syntax Description

| | |
|---|---|
| *cos_value* | Default CoS value for the interface; valid values are from 0 to 7. |

## Defaults

On non-Supervisor Engine 6-E supervisors the default CoS value is 0.

On the Supervisor Engine 6-E and Catalyst 4900M chassis the default CoS is implicitly set to 1.

**Note** CoS override is not configured.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

CoS values are configurable on physical LAN ports only.

## Examples

This example shows how to configure the default QoS CoS value as 6:

```
Switch(config-if)# qos cos 6
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| show qos | Displays QoS information. |

# qos dbl

To enable Dynamic Buffer Limiting (DBL) globally on the switch, use the **qos dbl** command. To disable DBL, use the **no** form of this command.

**qos dbl** [**buffers** {**aggressive-flow** *buffers*} | **credits** {**aggressive-flow** *credits* | **maximum** *max*} | **dscp-based** {*value* | *value range*} | **exceed-action** {**ecn** | **probability** *percent*} | **flow** {**include** [**layer4-ports**] [**vlan**]}]

**no qos dbl** [**buffers** {**aggressive-flow** *buffers*} | **credits** {**aggressive-flow** *credits* | **maximum** *max*} | **dscp-based** {*value* | *value range*} | **exceed-action** {**ecn** | **probability** *percent*} | **flow** {**include** [**layer4-ports**] [**vlan**]}]

## Syntax Description

| | |
|---|---|
| **buffers** | (Optional) Specifies the buffer limit for aggressive flows. |
| **aggressive-flow** | (Optional) Specifies the aggressive flow. |
| *buffers* | (Optional) Number of buffers for aggressive flows; valid values are from 0 to 255. |
| **credits** | (Optional) Specifies the credit limit for aggressive flows and all flows. |
| *credits* | (Optional) Number of credits for aggressive flows; valid values are from 0 to 15. |
| **maximum** | (Optional) Specifies the maximum credit for all flows. |
| *max* | (Optional) Number of credits for all flows; valid values are from 0 to 15. |
| **dscp-based** | (Optional) Specifies the packets that belong to the list of internal DSCPs. |
| *value* | (Optional) A single DSCP value; valid values are from 0 to 63. |
| *value range* | (Optional) A range of DSCP values; valid values are from 0 to 63. Up to 8 command separated DSCP values can be specified. |
| **exceed-action** | (Optional) Specifies the packet marking when the limits are exceeded. |
| **ecn** | (Optional) Specifies the explicit congestion notification. |
| **probability** | (Optional) Specifies the probability of packet marking. |
| *percent* | (Optional) Probability number; valid values are from 0 to 100. |
| **flow** | (Optional) Specifies the flows for limiting. |
| **include** | (Optional) Allows the Layer 4 ports and VLANs to be included in the flows. |
| **layer4-ports** | (Optional) Includes the Layer 4 ports in flows. |
| **vlan** | (Optional) Includes the VLANs in flows. |

## Defaults

On non-Supervisor Engine 6-E supervisors the default settings are as follows:

- QoS DBL is disabled.
- Aggressive-flow buffers is set to 2.
- Aggressive-flow credits is set to 2, with a limit of 10.
- Layer 4 ports are included.
- VLANs are included.
- 15 maximum credits are allowed.
- 15% drop probability is set.
- DSCP values are included.

On Supervisor Engine 6-E and Catalyst 4900M chassis supervisors the default dbl values are implicitly set and cannot be changed. The settings are as follows:

- seven maximum credits allowed.
- Aggressive-flow credits is set to 4.
- Aggressive-flow buffers is set to 4.
- six percent drop probability is set.
- Hash function for Layer 2 packets uses source and destination MAC addresses as well as transmit VLAN identifiers.
- Hash function for IPv4 and IPv6 packets uses source and destination IP addresses source and destination Layer 4 ports as well as transmit VLAN identifiers.

## Command Modes

Global configuration mode

QoS policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(13)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(37)SG | Added support for DSCP-based flow management. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

## Examples

This example shows how to enable DBL globally on the switch:

```
Switch(config)# qos dbl
Global DBL enabled
Switch(config)#
```

This example shows how to enable DBL in the QoS policy-map class configuration mode:

```
Switch(config)# class-map c1
Switch(config-cmap)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)#
```

This example shows how to selectively enable DBL on DSCP values 1 through 10:

```
Switch# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# qos dbl dscp-based 1-10
Switch(config)# end
Switch# show qos dbl
    DBL flow includes vlan
    DBL flow includes layer4-ports
    DBL does not use ecn to indicate congestion
    DBL exceed-action probability: 15%
    DBL max credits: 15
    DBL aggressive credit limit: 10
    DBL aggressive buffer limit: 2 packets
    DBL DSCPs with default drop probability:
```

```
        1-10
```

This example shows how to selectively disable DBL on DSCP values 1 through 10:

```
Switch# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no qos dbl dscp-based 1-5, 7
Switch(config)# end
Switch# show qos dbl
    DBL flow includes vlan
    DBL flow includes layer4-ports
    DBL does not use ecn to indicate congestion DBL exceed-action probability: 15% DBL max
    credits: 15 DBL aggressive credit limit: 10 DBL aggressive buffer limit: 2 packets DBL
    DSCPs with default drop probability:
         0,6,8-63
```

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

## Related Commands

| Command | Description |
|---|---|
| **show qos dbl** | Displays QoS Dynamic Buffer Limiting (DBL) information. |

# qos dscp

To define the default CoS value for an interface, use the **qos dscp** command. To remove a prior entry, use the **no** form of this command.

**qos dscp** *dscp_value*

**no qos dscp** *dscp_value*

## Syntax Description

| | |
|---|---|
| *dscp_value* | Default DSCP value for the interface; valid values are from 0 to 63. |

## Defaults

On non-Supervisor Engine 6-E supervisors the default DSCP value is 0.

On Supervisor Engine 6-E and Catalyst 4900M chassis supervisors the port DSCP value is always set to 0.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

## Examples

This example shows how to configure the default QoS DSCP value as 6:

```
Switch(config-if)# qos dscp 6
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show qos interface** | Displays QoS information for an interface. |

# qos map cos

To define the ingress CoS-to-DSCP mapping for the trusted interfaces, use the **qos map cos to dscp** command. To remove a prior entry, use the **no** form of this command.

**Note** You cannot remove a single entry from the table.

**qos map cos** *cos_values* **to dscp** *dscp1*

**no qos map cos to dscp**

## Syntax Description

| | |
|---|---|
| *cos_values* | CoS values; list up to eight CoS values separated by spaces. |
| **to dscp** | Defines mapping and specifies DSCP value. |
| *dscp1* | DSCP value to map to the CoS values; valid values are from 0 to 63. |

## Defaults

The default CoS-to-DSCP configuration settings are shown in the following table:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **CoS** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **DSCP** | 0 | 8 | 16 | 24 | 32 | 40 | 48 | 56 |

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. In place of this limited map capability, the Supervisor Engine 6-E and Catalyst 4900M chassis supports the setting of various marking fields in a packet within a policy map. Please refer to the **set** command for more details.

The CoS-to-DSCP map is used to map the packet CoS (on the interfaces that are configured to trust CoS) to the internal DSCP value. This map is a table of eight CoS values (0 through 7) and their corresponding DSCP values. The switch has one map.

## Examples

This example shows how to configure the ingress CoS-to-DSCP mapping for CoS 0:

```
Switch(config)# qos map cos 0 to dscp 20
Switch(config)#
```

This example shows how to clear the entire CoS-to-DSCP mapping table:

```
Switch(config)# no qos map cos 0 to dscp 20
```

```
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **qos map dscp** | Maps the DSCP values to selected transmit queues and to map the DSCP-to-CoS value. |
| **qos map dscp policed** | Sets the mapping of the policed DSCP values to the marked-down DSCP values. |
| **show qos** | Displays QoS information. |
| **tablemap** (refer to Cisco IOS documentation) | Modifies metric and tag values when the IP routing table is updated with BGP learned routes. |

# qos map dscp

To map the DSCP values to selected transmit queues and to map the DSCP-to-CoS value, use the **qos map dscp** command. To return to the default value, use the **no** form of this command.

**qos map dscp** *dscp-values* **to tx-queue** *queue-id*

**no qos map dscp** *dscp-values* **to cos** *cos-value*

## Syntax Description

| | |
|---|---|
| *dscp-values* | List of DSCP values to map to the queue ID; valid values are from 0 to 63. |
| **to** | Defines mapping. |
| **tx-queue** | Specifies a transmit queue. |
| *queue-id* | Transmit queue; valid values are from 1 to 4. |
| **cos** | Specifies the CoS value. |
| *cos-value* | Class of service; valid values are from 1 to 7. |

## Defaults

The default DSCP-to-CoS configuration settings are shown in the following table:

| **DSCP** | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |
|---|---|---|---|---|---|---|---|---|
| **CoS** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. In place of this command the Supervisor Engine 6-E and Catalyst 4900M chassis uses the **tablemap** command for QoS marking. Please refer to the **tablemap** command for details.

You use the DSCP-to-CoS map to map the final DSCP classification to a final CoS. The CoS map is written into the ISL header or 802.1Q tag of the transmitted packet on trunk interfaces and contains a table of 64 DSCP values and the corresponding CoS values. The switch has one map. You can enter up to eight DSCP values, separated by spaces, for a CoS value.

The DSCP-to-transmit-queue map is used to map the final DSCP classification to a transmit queue. You can enter up to eight DSCP values, separated by spaces, for a transmit queue.

## Examples

This example shows how to configure the egress DSCP-to-CoS mapping:

```
Switch(config)# qos map dscp 20 25 to cos 3
Switch(config)#
```

This example shows how to configure the egress DSCP-to-transmit queue:

```
Switch(config)# qos map dscp 20 25 to tx-queue 1
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **qos map cos** | Defines the ingress CoS-to-DSCP mapping for the trusted interfaces. |
| **show qos interface** | Displays queueing information. |
| **show qos** | Displays QoS information. |
| **tablemap** (refer to Cisco IOS documentation) | Modifies metric and tag values when the IP routing table is updated with BGP learned routes. |
| **tx-queue** | Configures the transmit queue parameters for an interface. |

# qos map dscp policed

To set the mapping of the policed DSCP values to the marked-down DSCP values, use the **qos map dscp policed** command. To remove a prior entry, use the **no** form of this command.

**qos map dscp policed** *dscp_list* **to dscp** *policed_dscp*

**no qos map dscp policed**

## Syntax Description

| | |
|---|---|
| *dscp_list* | DSCP values; valid values are from 0 to 63. |
| **to dscp** | Defines mapping. |
| *policed_dscp* | Marked-down DSCP values; valid values are from 0 to 63. |

## Defaults

Mapping of DSCP values is disabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. Various policer types are supported on the Supervisor Engine 6-E and Catlyst 4900M chassis that supports explicit QoS marking of DSCP, precedence, and CoS fields. Refer to the **police** command for details.

The DSCP-to-policed-DSCP map determines the marked-down DSCP value that is applied to the out-of-profile flows. The switch has one map.

You can enter up to eight DSCP values, separated by spaces.

You can enter only one policed DSCP value.

**Note** To avoid out-of-sequence packets, configure the DSCP-to-policed-DSCP map so that marked-down packets remain in the same queue as in-profile traffic.

## Examples

This example shows how to map multiple DSCPs to a single policed-DSCP value:

```
Switch(config)# qos map dscp policed 20 25 43 to dscp 4
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| qos map cos | Defines the ingress CoS-to-DSCP mapping for the trusted interfaces. |
| qos map dscp | Maps the DSCP values to selected transmit queues and to map the DSCP-to-CoS value. |
| show qos | Displays QoS information. |

# qos rewrite ip dscp

To enable DSCP rewrite for IP packets, use the **qos rewrite ip dscp** command. To disable IP DSCP rewrite, use the **no** form of this command.

**qos rewrite ip dscp**

**no qos rewrite ip dscp**

## Syntax Description

This command has no arguments or keywords.

## Defaults

IP DSCP rewrite is enabled.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

If you disable IP DSCP rewrite and enable QoS globally, the following events occur:

- The ToS byte on the IP packet is not modified.
- Marked and marked-down DSCP values are used for queueing.
- The internally derived DSCP (as per the trust configuration on the interface or VLAN policy) is used for transmit queue and Layer 2 CoS determination. The DSCP is not rewritten on the IP packet header.

If you disable QoS, the CoS and DSCP of the incoming packet are preserved and are not rewritten.

## Examples

This example shows how to disable IP DSCP rewrite:

```
Switch(config)# no qos rewrite ip dscp
Switch(config)#
```

## Related Commands

| Command | Description |
|---|---|
| qos (global configuration mode) | Enables QoS functionality on the switch. |
| show qos | Displays QoS information. |

# qos trust

To set the trusted state of an interface (for example, whether the packets arriving at an interface are trusted to carry the correct CoS, ToS, and DSCP classifications), use the **qos trust** command. To set an interface to the untrusted state, use the **no** form of this command.

**qos trust** {**cos** | *device cisco-phone* | **dscp** | **extend** [**cos** *priority*]}

**no qos trust** {**cos** | *device cisco-phone* | **dscp** | **extend** [**cos** *priority*]}

## Syntax Description

| | |
|---|---|
| **cos** | Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits. |
| *device cisco-phone* | Specifies the Cisco IP phone as the trust device for a port. |
| **dscp** | Specifies that the ToS bits in the incoming packets contain a DSCP value. |
| **extend** | Specifies to extend the trust to Port VLAN ID (PVID) packets coming from the PC. |
| **cos** *priority* | (Optional) Specifies that the CoS priority value is set to PVID packets; valid values are from 0 to 7. |

## Defaults

The default settings are as follows:

- If global QoS is enabled, trust is disabled on the port.
- If global QoS is disabled, trust DSCP is enabled on the port.
- The CoS priority level is 0.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.1(11)EW | Support for extending trust for voice was added. |
| 12.1(19)EW | Support for trust device Cisco IP phone was added. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

You can only configure the trusted state on physical LAN interfaces.

By default, the trust state of an interface when QoS is enabled is untrusted; when QoS is disabled on the interface, the trust state is reset to trust DSCP.

When the interface trust state is **qos trust cos**, the transmit CoS is always the incoming packet CoS (or the default CoS for the interface, if the packet is not tagged).

When the interface trust state is not **qos trust dscp**, the security and QoS ACL classification will always use the interface DSCP and not the incoming packet DSCP.

Trusted boundary should not be configured on the ports that are part of an EtherChannel (that is, a port channel).

## Examples

This example shows how to set the trusted state of an interface to CoS:

```
Switch(config-if)# qos trust cos
Switch(config-if)#
```

This example shows how to set the trusted state of an interface to DSCP:

```
Switch(config-if)# qos trust dscp
Switch(config-if)#
```

This example shows how to set the PVID CoS level to 6:

```
Switch(config-if)# qos trust extend cos 6
Switch(config-if)#
```

This example shows how to set the Cisco phone as the trust device:

```
Switch(config-if)# qos trust device cisco-phone
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| qos cos | Defines the default CoS value for an interface. |
| qos vlan-based | Defines per-VLAN QoS for a Layer 2 interface. |
| show qos interface | Displays QoS information for an interface. |

# qos vlan-based

To enable per-VLAN QoS for a Layer 2 interface, use the **qos vlan-based** command. To disable per-VLAN QoS for a Layer 2 interface, use the **no** form of this command.

**qos vlan-based**

**no qos vlan-based**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Per-VLAN QoS is disabled.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis. On the Supervisor Engine 6-E and Catalyst 4900M chassis various QoS marking and policing actions at the interface and VLAN level are appropriately merged. For details, refer to the *Catalyst 4500 Series Switch Configuration Guide*.

In VLAN-based mode, the policy map that is attached to the Layer 2 interface is ignored, and QoS is driven by the policy map that is attached to the corresponding VLAN interface.

Per-VLAN QoS can be configured only on the Layer 2 interfaces.

If no input QoS policy is attached to a Layer 2 interface, then the input QoS policy that is attached to the VLAN (on which the packet is received), if any, is used even if the port is not configured as VLAN based.

If you do not want this default, attach a placeholder input QoS policy to the Layer 2 interface.

Similarly, if no output QoS policy is attached to a Layer 2 interface, then the output QoS policy that is attached to the VLAN (on which the packet is transmitted), if any, is used even if the port is not configured as VLAN based.

If you do not want this default, attach a placeholder output QoS policy to the Layer 2 interface.

Layer 3 interfaces are always in interface-based mode. Layer 3 VLAN interfaces are always in VLAN-based mode.

## Examples

This example shows how to enable per-VLAN QoS for a Layer 2 interface:

```
Switch(config-if)# qos vlan-based
Switch(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| qos cos | Defines the default CoS value for an interface. |
| show qos interface | Displays QoS information for an interface. |

# queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** command. To remove the queue packet limit from a class, use the **no** form of this command.

**queue-limit** *number-of-packets*

**no queue-limit** *number-of-packets*

## Syntax Description

| | |
|---|---|
| *number-of-packets* | Number of packets that the queue for this class can accumulate; valid range is 16 to 8184. This number must be a multiple of 8. |

## Defaults

By default, each physical interface on a Catalyst 4500 switch has a default queue based on the number of slots in a chassis and the number of ports on the linecards.

## Command Modes

QoS policy-map class configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SG | This command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This class-based queuing (CBQ) command applies only to the Supervisor 6E as part of the MQC support on the Catalyst 4500 supervisor.

By default, each physical interface on a Catalyst 4500 switch comes up with a default queue. The size of this queue is based on the number of slots in a chassis as well as the number of ports on the line card in each slot. The switch supports 512K queue entries of which 100K are set aside as a common sharable pool. The remaining 412K entries are equally distributed among the slots. Each slot further divides its allocated queue entries equally among its ports.

CBQ creates a queue for every class for which a class map is defined. Packets satisfying the match criterion for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop or, if DBL is configured for the class policy, packet drop to take effect.

**Note** The queue-limit command is supported only after you first configure a scheduling action, such as bandwidth, shape, or priority, except when you configure queue-limit in the class-default class of an output QoS policy-map.s

## Examples

This example shows how to configure a policy-map called *policy11* to contain policy for a class called *acl203*. Policy for this class is set so that the queue reserved for it has a maximum packet limit of 40:

```
Switch# configure terminal
Switch (config)# policy-map policy11
Switch (config-pmap)# class acl203
Switch (config-pmap-c)# bandwidth 2000
Switch (config-pmap-c)# queue-limit 40
Switch (config-pmap-c)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port. |
| **class** | Specifies the name of the class whose traffic policy you want to create or change. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **shape (class-based queueing)** | Enables traffic shaping a class of traffic in a policy map attached to a physical port. |

# redundancy

To enter the redundancy configuration mode, use the **redundancy** command in the global configuration mode.

**redundancy**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only). |

## Usage Guidelines

The redundancy configuration mode is used to enter the main CPU submode.

To enter the main CPU submode, use the **main-cpu** command in the redundancy configuration mode.

The main CPU submode is used to manually synchronize the configurations on the two supervisor engines.

From the main CPU submode, use the **auto-sync** command to enable automatic synchronization of the configuration files in NVRAM.

Use the **no** command to disable redundancy. If you disable redundancy, then reenable redundancy, the switch returns to default redundancy settings.

Use the **exit** command to exit the redundancy configuration mode.

## Examples

This example shows how to enter redundancy mode:

```
Switch(config)# redundancy
Switch(config-red)#
```

This example shows how to enter the main CPU submode:

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)#
```

## Related Commands

| Command | Description |
|---|---|
| auto-sync | Enables automatic synchronization of the configuration files in NVRAM. |
| main-cpu | Enters the main CPU submode and manually synchronize the configurations on the two supervisor engines. |

# redundancy config-sync mismatched-commands

If your active and standby supervisors are running different versions of IOS, some of their CLIs will not be compatible. If such commands are already present in the running configuration of the active supervisor engine and the syntax-check for the command fails at the standby supervisor engine while it is booting, the **redundancy config-sync mismatched-commands** command moves the active supervisor engine into the Mismatched Command List (MCL) and resets the standby supervisor engine.

**redundancy config-sync** {**ignore** | **validate**} **mismatched-commands**

## Syntax Description

| | |
|---|---|
| **ignore** | Ignore the mismatched command list. |
| **validate** | Revalidate the mismatched command list with the modified running-configuration. |

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SGA | This command was introduced on the Catalyst 4500 series switch. |
| 12.2(44)SG | Updated command syntax from issu config-sync to redundancy config-sync. |

## Usage Guidelines

The following is a log entry example for mismatched commands:

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
  show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
 ! <submode> "interface"
- ip address 11.0.0.1 255.0.0.0
 ! </submode> "interface"
```

To display all mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

**Step 1** Remove all mismatched commands from the active supervisor engine's running configuration.

**Step 2** Revalidate the MCL with a modified running configuration using the **redundancy config-sync validate mismatched-commands** command.

**Step 3** Reload the standby supervisor engine.

You could also ignore the MCL by doing the following:

**Step 1** Enter the **redundancy config-sync ignore mismatched-commands** command.

**Step 2** Reload the standby supervisor engine; the system changes to SSO mode.

**Note** If you ignore the mismatched commands, the *out-of-sync* configuration at the active supervisor engine and the standby supervisor engine still exists.

**Step 3** You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

When an ISSU/SSO MCL failure occurs, the peer image is placed in an incompatible list. Even if the configuration is corrected and synchronized to the other switch, subsequent reloads will not establish SSO because of the image's membership on this list. To clear the peer image incompatibility status, enter the **redundancy config-sync ignore mismatched-command**s command while the peer is in a standby cold state.

## Examples

This example shows how you can validate removal of entries from the MCL:

```
Switch# redundancy config-sync validate mismatched-commands
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| show redundancy config-sync | Displays an ISSU config-sync failure or the ignored mismatched command list (MCL). |

# redundancy force-switchover

To force a switchover from the active to the standby supervisor engine, use the **redundancy force-switchover** command.

**redundancy force-switchover**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only). |

## Usage Guidelines

Before using this command, refer to the "Performing a Software Upgrade" section of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional information.

The **redundancy force-switchover** command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the Cisco IOS image. The modules are reset.

The old active supervisor engine reboots with the new image and becomes the standby supervisor engine.

## Examples

This example shows how to switch over manually from the active to the standby supervisor engine:

```
Switch# redundancy force-switchover
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| redundancy | Enters the redundancy configuration mode. |
| show redundancy | Displays redundancy facility information. |

# redundancy reload

To force a reload of one or both supervisor engines, use the **redundancy reload** command.

**redundancy reload** {**peer** | **shelf**}

## Syntax Description

| | |
|---|---|
| **peer** | Reloads the peer unit. |
| **shelf** | Reboots both supervisor engines. |

## Defaults

This command has no default settings.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only). |

## Usage Guidelines

Before using this command, refer to the "Performing a Software Upgrade" section of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional information.

The **redundancy reload shelf** command conducts a reboot of both supervisor engines. The modules are reset.

## Examples

This example shows how to manually reload one or both supervisor engines:

```
Switch# redundancy reload shelf
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **redundancy** | Enters the redundancy configuration mode. |
| **show redundancy** | Displays redundancy facility information. |

# remote login module

To remotely connect to a specific module, use the **remote login module** configuration command.

**remote login module** *mod*

## Syntax Description

| | |
|---|---|
| *mod* | Target module for the command. |

## Defaults

This command has no default settings.

## Command Modes

Privileged

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command applies only to the Access Gateway Module on Catalyst 4500 series switches.

The valid values for *mod* depends on the chassis used. For example, if you have a Catalyst 4506 chassis, valid values for the module are from 2 to 6. If you have a 4507R chassis, valid values are from 3 to 7.

When you execute the **remote login module** *mod* command, the prompt changes to Gateway#

The **remote login module** command is identical to the **session module** *mod* and the **attach module** *mod* commands.

## Examples

This example shows how to remotely log in to the Access Gateway Module:

```
Switch# remote login module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

## Related Commands

| Command | Description |
|---|---|
| attach module | Remotely connects to a specific module. |
| session module | Logs in to the standby supervisor engine using a virtual console. |

# remote-span

To convert a VLAN into an RSPAN VLAN, use the **remote-span** command. To convert an RSPAN VLAN to a VLAN, use the **no** form of this command.

**remote-span**

**no remote-span**

## Syntax Description

This command has no arguments or keywords.

## Defaults

RSPAN is disabled.

## Command Modes

VLAN configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(20)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to convert a VLAN into an RSPAN VLAN:

```
Switch# config terminal
Switch(config)# vlan 20
Switch(config-vlan)# remote-span
Switch(config-vlan)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| monitor session | Enables the SPAN sessions on interfaces or VLANs. |

# renew ip dhcp snooping database

To renew the DHCP binding database, use the **renew ip dhcp snooping database** command.

**renew ip dhcp snooping database** [**validation none**] [**url**]

## Syntax Description

| | |
|---|---|
| **validation none** | (Optional) Specifies that the checksum associated with the contents of the file specified by the URL is not verified. |
| **url** | (Optional) Specifies the file from which the read is performed. |

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.1(19)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If the URL is not provided, the switch tries to read the file from the configured URL.

## Examples

This example shows how to renew the DHCP binding database while bypassing the CRC checks:

```
Switch# renew ip dhcp snooping database validation none
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping. |
| **ip dhcp snooping binding** | Sets up and generates a DHCP binding configuration to restore bindings across reboots. |
| **ip dhcp snooping information option** | Enables DHCP option 82 data insertion. |
| **ip dhcp snooping trust** | Enables DHCP snooping on a trusted VLAN. |
| **ip dhcp snooping vlan** | Enables DHCP snooping on a VLAN or a group of VLANs. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding entries. |

# reset

To leave the proposed new VLAN database but remain in VLAN configuration mode and reset the proposed new database to be identical to the VLAN database currently implemented, use the **reset** command.

**reset**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command has no default settings.

## Command Modes

VLAN configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Examples

This example shows how to reset the proposed new VLAN database to the current VLAN database:

```
Switch(vlan-config)# reset
RESET completed.
Switch(vlan-config)#
```

# revision

To set the MST configuration revision number, use the **revision** command. To return to the default settings, use the **no** form of this command.

**revision** *version*

**no revision**

## Syntax Description

| | |
|---|---|
| *version* | Configuration revision number; valid values are from 0 to 65535. |

## Defaults

Revision version is set to 0.

## Command Modes

MST configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

If two Catalyst 4500 series switches have the same configuration but have different configuration revision numbers, they are considered to be part of two different regions.

**Caution** Be careful when using the **revision** command to set the MST configuration revision number because a mistake can put the switch in a different region.

## Examples

This example shows how to set the configuration revision number:

```
Switch(config-mst)# revision 5
Switch(config-mst)#
```

## Related Commands

| Command | Description |
|---|---|
| **instance** | Maps a VLAN or a set of VLANs to an MST instance. |
| **name** | Sets the MST region name. |
| **show spanning-tree mst** | Displays MST protocol information. |
| **spanning-tree mst configuration** | Enters the MST configuration submode. |

# redundancy config-sync mismatched-commands

To move the active supervisor engine into the Mismatched Command List (MCL) and resets the standby supervisor engine, use the **redundancy config-sync mismatched-commands** command.

If your active and standby supervisors engines are running different versions of Cisco IOS, some of their CLIs will not be compatible. If such commands are already present in the running configuration of the active supervisor engine and the syntax-check for the command fails at the standby supervisor engine while it is booting, you must move the active supervisor engine into the Mismatched Command List (MCL).

**redundancy config-sync** {**ignore** | **validate**} **mismatched-commands**

## Syntax Description

| | |
|---|---|
| **ignore** | Ignore the mismatched command list. |
| **validate** | Revalidate the mismatched command list with the modified running-configuration. |

## Defaults

This command has no default settings.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SGA | This command was introduced on the Catalyst 4500 series switch. |
| 12.2(44)SG | Updated command name from **issu config-sync** to **redundancy config-sync**. |

## Usage Guidelines

The following is a log entry example for mismatched commands:

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
  show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
 ! <submode> "interface"
- ip address 11.0.0.1 255.0.0.0
 ! </submode> "interface"
```

To display all mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, remove all mismatched commands from the active supervisor engine's running configuration, revalidate the MCL with a modified running configuration using the **redundancy config-sync validate mismatched-commands** command, then reload the standby supervisor engine.

You could also ignore the MCL by entering the **redundancy config-sync ignore mismatched-commands** command and reloading the standby supervisor engine; the system changes to SSO mode.

**Note** If you ignore the mismatched commands, the *out-of-sync* configuration at the active supervisor engine and the standby supervisor engine still exists.

You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

If SSO mode cannot be established between the active and standby supervisor engines because of an incompatibility in the configuration file, a mismatched command list (MCL) is generated at the active supervisor engine and a reload into RPR mode is forced for the standby supervisor engine. Subsequent attempts to establish SSO, after removing the offending configuration and rebooting the standby supervisor engine with the exact same image, might cause the C4K_REDUNDANCY-2-IOS_VERSION_CHECK_FAIL and ISSU-3-PEER_IMAGE_INCOMPATIBLE messages to appear because the peer image is listed as incompatible. If the configuration problem can be corrected, you can clear the peer image from the incompatible list with the **redundancy config-sync ignore mismatched-commands** EXEC command while the peer is in a standby cold (RPR) state. This action allows the standy supervisor engine to boot in standby hot (SSO) state when it reloads.

## Examples

This example shows how to validate removal of entries from the MCL:

```
Switch# redundancy config-sync validate mismatched-commands
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| show redundancy config-sync | Displays an ISSU config-sync failure or the ignored mismatched command list (MCL). |

# service-policy (interface configuration)

To attach a policy map to an interface or to apply different QoS policies on VLANs that an interface belongs to, use the **service-policy** command. To remove a policy map from an interface, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| **input** | Specifies the input policy maps. |
| **output** | Specifies the output policy maps. |
| *policy-map name* | Name of a previously configured policy map. |

## Defaults

A policy map is not attached to an interface or a VLAN.

## Command Modes

Interface configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(25)EWA | Support for applying different QoS policies on VLANs was introduced. |

## Usage Guidelines

Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the **vlan-range** command, you can use the **service-policy** command to specify different QoS policies on different VLANs.

**Note** This capability is restricted to Layer 2 interfaces.

### Non-Supervisor Engine 6-E

You cannot apply a policy map under an interface and a VLAN range at the same time.

To attach a service policy to a VLAN an SVI must be created for the VLAN and the policy must be applied to the SVI.

### Supervisor Engine 6-E and Catalyst 4900M chassis

You can apply a service policy under an interface as well as a VLAN range at the same time. However, this is allowed only when the interface policy has only queuing actions whereas a VLAN has only non-queueing actions (QoS marking and/or policing) actions.

To attach a service policy to a VLAN, the VLAN configuration mode has to be used.

## Examples

This example shows how to attach a policy map to Fast Ethernet interface 5/20:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/20
Switch(config-if)# service-policy input pmap1
Switch(config-if)# end
```

This example shows how to apply policy map p1 for traffic in VLANs 20 and 400, and policy map p2 for traffic in VLANs 300 through 301:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan-range 20,400
Switch(config-if-vlan-range)# service-policy input p1
Switch(config-if-vlan-range)# exit
Switch(config-if)# vlan-range 300-301
Switch(config-if-vlan-range)# service-policy output p2
Switch(config-if-vlan-range)# end
Switch# show policy-map interface gigabitEthernet 6/1 vlan 20
 GigabitEthernet6/1 vlan 20

  Service-policy input: p1

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

Switch# show policy-map interface gigabitEthernet 6/1
 GigabitEthernet6/1 vlan 20

  Service-policy input: p1

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

 GigabitEthernet6/1 vlan 300

  Service-policy output: p2

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

 GigabitEthernet6/1 vlan 301

  Service-policy output: p2

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
```

```
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

 GigabitEthernet6/1 vlan 400

  Service-policy input: p1

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes
```

This example shows how to attach a policy map to a VLAN using an SVI on a non-Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)#interface vlan 10
Switch(config-if)#service-policy out policy-vlan
Switch(config-if)#end
Switch#
```

This example shows how to attach a policy map to a VLAN using a Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)#vlan configuration 20
Switch(config-vlan-config)#service-policy out policy-vlan
Switch(config-vlan-config)#end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| class-map | Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode. |
| policy-map | Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| service-policy (interface configuration) | Attaches a policy map to an interface. |
| show policy-map interface vlan | Displays the QoS policy-map information applied to a specific VLAN on an interface. |

# service-policy (policy-map class)

To create a service policy that is a quality of service (QoS) policy within a policy map (called a hierarchical service policy), use the **service-policy** policy-map class configuration command. To disable the service policy within a policy map, use the **no** form of this command.

**service-policy** *policy-map-name*

**no service-policy** *policy-map-name*

## Syntax Description

| | |
|---|---|
| *policy-map-name* | Name of the policy map. |

## Defaults

No service policies maps are defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(40)SG | Added support for Supervisor Engine 6-E and Catalyst 4900M chassis. |

## Usage Guidelines

Use the **service-policy** command only in a hierarchical policy map attached to a physical port. This command is valid in policy maps at level two of the hierarchy.

You can create a hierarchy by having the parent policy map specify marking and/or policing actions and having the child policy map specify the queueing actions.

If you enter this command in policy-map class configuration mode, you return to policy-map configuration mode by using the **exit** command. To return to privileged EXEC mode, use the **end** command.

## Examples

This example shows how to create a hierarchical service policy in the service policy called “parent”:

```
Switch# configure terminal
Switch(config)# policy-map child
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map parent
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 32k
Switch(config-pmap-c)# service-policy child
Switch#
```

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

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Creates a signaling class structure that can be referred to by its name. |
| **class** | Specifies the name of the class whose traffic policy you want to create or change. |
| **dbl** | Enables active queue management on a transmit queue used by a class of traffic. |
| **policy-map** | Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **priority** | Enables the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port. |
| **random-detect** (refer to Cisco IOS documentation) | Enables Weighted Random Early Detection (WRED) or distributed WRED (DWRED). |
| **shape (class-based queueing)** | Enables traffic shaping a class of traffic in a policy map attached to a physical port. |
| **show policy-map** | Displays information about the policy map. |

# service-policy input (control-plane)

To attach a policy map to a control plane for aggregate control plane services, use the **service-policy input** command. Use the **no** form of this command to remove a service policy from a control plane.

**service-policy input** *policy-map-name*

## Syntax Description

| | |
|---|---|
| **input** | Applies the specified service policy to the packets that are entering the control plane. |
| *policy-map-name* | Name of a service policy map (created using the **policy-map** command) to be attached. |

## Defaults

No service policy is specified.

## Command Modes

Control-plane configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

In this release, the only policy-map accepted on the control-plane is system-cpp-policy. It is already attached to the control-plane at start up. If not (due to some error conditions), it is recommended to use the **global macro system-cpp** command to attach it to the control-plane. The system-cpp-policy created by the system contains system pre-defined classes. For these pre-defined classes, you can change the policing parameters but you should not make any other change to the classes.

You can define your own class-maps and append them to the end of the system-cpp-policy policy-map.

## Examples

This example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate:

```
Switch(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Switch(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Switch(config)# class-map telnet-class
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map control-plane-policy
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c)# police 80000 conform transmit exceed drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor.
```

```
Switch(config)# control-plane
Switch(config-cp)# service-policy input control-plane-policy
Switch(config-cp)# exit
```

## Related Commands

| Command | Description |
|---|---|
| control-plane | Enters control-plane configuration mode. |
| macro global apply system-cpp | Applies the control plane policing default template to the switch. |
| policy-map | Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| show policy-map control-plane | Displays the configuration either of a class or of all classes for the policy map of a control plane. |

# session module

**Note** This command is only supported in SSO mode and does not work in RPR mode.

To login to the standby supervisor engine using a virtual console, use the **session module** configuration command.

**session module** *mod*

## Syntax Description

| | |
|---|---|
| *mod* | Target module for the command. |

## Defaults

This command has no default settings.

## Command Modes

Privileged

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SG | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

Catalyst 4500 series switches can be configured with 2 supervisor engines to provide redundancy. When the switch is powered, one of the supervisor engines becomes active and remains active until a switchover occurs. The other supervisor engine remains in standby mode.

Each supervisor engine has its own console port. Access to the standby supervisor engine is possible only through the console port of the standby supervisor engine. Therefore, you must connect to the standby console to access, monitor or debug the standby supervisor.

Virtual Console for Standby Supervisor Engine enables you to access the standby console from the active supervisor engine without requiring a physical connection to the standby console. It uses IPC over EOBC to communicate with the standby supervisor engine and thus emulate the standby console on the active supervisor engine. Only one active standby console session is active at any time.

The Virtual Console for Standby Supervisor Engine allows users who are logged onto the active supervisor engine to remotely execute show commands on the standby supervisor engine and view the results on the active supervisor engine. Virtual Console is available only from the active supervisor engine.

You can access the standby virtual console from the active supervisor engine with the **attach module**, **session module**, or **remote login** commands on the active supervisor engine. You must be in privilege EXEC mode (level 15) to run these commands to access the standby console.

**Note** The **session module** command is identical to the **attach module** *mod* and the **remote login module** *mod* commands.

Once you enter the standby virtual console, the terminal prompt automatically changes to "<hostname>-standby-console#" where hostname is the configured name of the switch. The prompt is restored back to the original prompt when you exit the virtual console.

You exit the virtual console with the **exit** or **quit** commands. When the inactivity period of the terminal on the active supervisor engine where you logged in exceeds the configured idle time, you are automatically logged out of the terminal on the active supervisor engine. In such a case, the virtual console session is also terminated. Virtual console session is also automatically terminated when the standby is rebooted. After the standby boots up, you need to create another virtual console session.

The following limitations apply to the standby virtual console:

All commands on the virtual console run to completion. It does not provide the auto-more feature; it behaves as if the **terminal length 0** command has been executed. It is also non-interactive. Therefore, a running command cannot be interrupted or aborted by any key sequence on the active supervisor engine. Therefore if a command produces considerable output, the virtual console displays it on the supervisor screen.

The virtual console is non-interactive. Because the virtual console does not detect the interactive nature of a command, any command that requires user interaction causes the virtual console to wait until the RPC timer aborts the command.

The virtual console timer is set to 60 seconds. The virtual console returns to its prompt after 60 seconds. During this time, you cannot abort the command from the key board. You must wait for the timer to expire before you continue.

You cannot use virtual console to view debug and syslog messages that are being displayed on the standby supervisor engine. The virtual console only displays the output of commands that are executed from the virtual console. Other information that is displayed on the real standby console does not appear on the virtual console.

## Examples

To login to the standby supervisor engine using a virtual console, do the following:

```
Switch# session module 2
Connecting to standby virtual console
Type "exit" or "quit" to end this session

Switch-standby-console# exit
Switch#
```

If the standby console is not enabled, the following message appears.

```
Switch-standby-console#
Standby console disabled.
Valid commands are: exit, logout
```

## Related Commands

| Command | Description |
|---|---|
| attach module | Remotely connects to a specific module. |
| remote login module | Remotely connects to a specific module. |

# set

To mark IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet, use the **set** policy-map class configuration command. To remove the traffic classification, use the **no** form of this command.

**set** {**cos** *new-cos* | [**ip**] {**dscp** *new-dscp* | **precedence** *new-precedence*} | **qos group** *value*}

**no set cos** *new-cos* | **ip** {**dscp** *new-dscp* | **precedence** *new-precedence*} | **qos group** *value*}

## Syntax Description

| | |
|---|---|
| **cos** *new-cos* | New CoS value assigned to the classified traffic. The range is 0 to 7. |
| **ip dscp** *new-dscp* | New DSCP value assigned to the classified traffic. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. The specified value sets the type of service (ToS) traffic class byte in the IPv4/IPv6 packet header. |
| **ip precedence** *new-precedence* | New IP-precedence value assigned to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. The specified value sets the precedence bit in the IP header. |
| **qos group** *value* | Internal QoS group assigned to a classified packet on ingress to an interface. |

## Defaults

No marking is enabled on packets.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(40)SG | Added support for Supervisor Engine 6-E and Catalyst 4900M chassis. |

## Usage Guidelines

You can use the **set** command only in class-level classes.

The **set dscp** *new-dscp* and the **set precedence** *new-precedence* commands are the same as the **set ip dscp** *new-dscp* and the **set ip precedence** *new-precedence* commands.

For the **set dscp** *new-dscp* or the **set precedence** *new-precedence* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the as same entering the **set dscp 10** command. You can enter the **set precedence critical** command, which is the same as entering the **set precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set precedence ?** command to see the command-line help strings.

You can configure the **set cos** *new-cos*, **set dscp** *new-dscp*, or **set precedence** *new-precedence* command in an ingress and an egress policy map attached to an interface or VLAN.

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

## Examples

This example shows how to create a policy map called *p1* with CoS values assigned to different traffic types. Class maps for "voice" and "video-data" have already been created.

```
Switch# configure terminal
Switch(config)# policy-map p1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap)# exit
Switch#
```

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

## Related Commands

| Command | Description |
|---|---|
| **class** | Specifies the name of the class whose traffic policy you want to create or change. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **show policy-map** | Displays information about the policy map. |
| **trust** | Defines a trust state for traffic classified through the **class** policy-map configuration command. |

# set cos

To set the Layer 2 class of service (CoS) value of a packet, use the **set cos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| *cos-value* | Specific IEEE 802.1Q CoS value from 0 to 7. |
| *from-field* | Specific packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:<br>• **precedence**<br>• **dscp**<br>• **cos**<br>• **qos group** |
| **table** | (Optional) Indicates that the values set in a specified table map will be used to set the CoS value. |
| *table-map-name* | (Optional) Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters. |

## Command Default

No CoS value is set for the outgoing packet.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M chassis. |

## Usage Guidelines

The **set cos** command can be used in an ingress as well as an egress policy map attached to an interface or VLAN.

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the CoS value. The "from-field" packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)
- Cost of Service (CoS)
- Quality of Service (QoS) group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the CoS value. For instance, if you configure the **set cos precedence** command, the precedence value will be copied and used as the CoS value.

You can do the same for the DSCP marking category. That is, you can configure the **set cos dscp** command, and the DSCP value will be copied and used as the CoS value.

**Note** If you configure the **set cos dscp** command, only the *first three bits* (the class selector bits) of the DSCP field are used.

**Note** If you configure the **set cos qos group** command, only the three least significant bits of the qos group field are used.

## Examples

This example shows how to configure a policy map called "cos-set" and assign different CoS values for different types of traffic. This example assumes that the class maps called "voice" and "video-data" have already been created.

```
Switch# configure terminal
Switch(config)# policy-map cos-set
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap-c)# end
Switch#
```

This example shows how to configure a policy map called "policy-cos" and to use the values defined in a table map called "table-map1". The table map called "table-map1" was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

This example shows how the setting of the CoS value is based on the precedence value defined in "table-map1":

```
Switch# configure terminal
Switch(config)# policy-map policy-cos
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos precedence table table-map1
Switch(config-pmap-c)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| match (class-map configuration) | Defines the match criteria for a class map. |
| policy-map | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| service-policy (policy-map class) | Creates a service policy that is a quality of service (QoS) policy within a policy map. |

| Command | Description |
|---|---|
| set dscp | Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte. |
| set precedence | Sets the precedence value in the packet header. |
| show policy-map | Displays information about the policy map. |

# set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| **ip** | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. |
| *dscp-value* | A number from 0 to 63 that sets the DSCP value. A mnemonic name for commonly used values can also be used. |
| *from-field* | Specific packet-marking category to be used to set the DSCP value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:<br>• **cos**<br>• **qos-group**<br>• **dscp**<br>• **precedence** |
| **table** | (Optional) Used in conjunction with the *from-field* argument. Indicates that the values set in a specified table map will be used to set the DSCP value. |
| *table-map-name* | (Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters. |

## Command Default

Disabled

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(40)SG | Added support for 'from-field' for policy-map configured on a Supervisor Engine 6-E. |

## Usage Guidelines

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

### DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group
- Precedence
- Differentiated services code point (DSCP)

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the "from-field" category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.

**Note** The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 63.

### Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those which meet the match criteria of the class-map containing this function.

### Set DSCP Values for IPv6 Packets Only

To set DSCP values for IPv6 values only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

### Set DSCP Values for IPv4 Packets Only

To set DSCP values for IPv4 packets only, use the **ip** keyword in the **match** command for classification. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

## Examples

### Packet-marking Values and Table Map

In the following example, the policy map called "policy1" is created to use the packet-marking values defined in a table map called "table-map1". The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the table-map (value mapping) command page.

This example shows how the DSCP value is set according to the CoS value defined in the table map called "table-map1".

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp cos table table-map1
Switch(config-pmap-c)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **match (class-map configuration)** | Defines the match criteria for a class map. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **service-policy (policy-map class)** | Creates a service policy that is a quality of service (QoS) policy within a policy map. |
| **set cos** | Sets IP traffic by setting a class of service (CoS). |
| **set precedence** | Sets the precedence value in the packet header. |
| **show policy-map** | Displays information about the policy map. |
| **show policy-map interface** | Displays the statistics and configurations of the input and output policies that are attached to an interface. |
| **table-map (value mapping)** (refer to Cisco IOS documentation) | Modifies metric and tag values when the IP routing table is updated with BGP learned routes. |

# set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| *precedence-value* | A number from 0 to 7 that sets the precedence bit in the packet header. |
| *from-field* | Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this argument value establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:<br>• **cos**<br>• **qos-group**<br>• **dscp**<br>• **precedence** |
| **table** | (Optional) Indicates that the values set in a specified table map will be used to set the precedence value. |
| *table-map-name* | (Optional) Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters. |

## Command Default

Disabled

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8a)EW | Support for this command was introduced on the Catalyst 4500 series switch. |
| 12.2(40)SG | Added support for 'from-field' for policy-map configured on a Supervisor Engine 6-E. |

## Usage Guidelines

### Command Compatibility

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can be one value or the other, but not both.

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the precedence value. The "from-field" packet-marking categories are as follows:

- CoS
- QoS group
- DSCP
- Precedence

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the "from-field" category as the precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 63. Therefore, when configuring the **set precedence qos-group** command the three least significant bits of qos-group are copied to precedence.

#### Precedence Values in IPv6 Environments

When this command is used in IPv6 environments it can set the value in both IPv4 and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class-map containing this function.

#### Setting Precedence Values for IPv6 Packets Only

To set the precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used in the class-map that classified packets for this action. Without the **match protocol ipv6** command, the class-map may classify both IPv6 and IPv4 packets, (depending on other match criteria) and the **set precedence** command will act upon both types of packets.

#### Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence** or **set dscp** command may act upon both types of packets.

## Examples

In the following example, the policy map named policy-cos is created to use the values defined in a table map named table-map1. The table map named table-map1 was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

This example shows how the precedence value is set according to the CoS value defined in table-map1.

```
Switch# configure terminal
Switch(config)# policy-map policy-cos
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set precedence cos table table-map1
Switch(config-pmap-c)# end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| **match (class-map configuration)** | Defines the match criteria for a class map. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **service-policy (policy-map class)** | Creates a service policy that is a quality of service (QoS) policy within a policy map. |
| **set cos** | Sets IP traffic by setting a class of service (CoS). |
| **set dscp** | Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte. |
| **set qos-group** | Sets a quality of service (QoS) group identifier (ID) that can be used later to classify packets. |
| **set precedence** | Sets the precedence value in the packet header. |
| **show policy-map** | Displays information about the policy map. |
| **show policy-map interface** | Displays the statistics and configurations of the input and output policies that are attached to an interface. |
| **table-map (value mapping)** (refer to Cisco IOS documentation) | Modifies metric and tag values when the IP routing table is updated with BGP learned routes. |

# set qos-group

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

**set qos-group** *group-id*

**no set qos-group** *group-id*

## Syntax Description

| | |
|---|---|
| *group-id* | Group ID number in the range from 0 to 63. |

## Command Default

The group ID is set to 0.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M chassis. |

## Usage Guidelines

The **set qos-group** command allows you to associate a group ID with a packet. This association is made through a service-policy attached to an interface or VLAN in the input direction. The group ID can be later used in the output direction to apply QoS service policies to the packet.

## Examples

This example shows how to set the qos-group to 5:

```
Switch#configure terminal
Switch(config)#policy-map p1
Switch(config-pmap)#class c1
Switch(config-pmap-c)#set qos
Switch(config-pmap-c)#set qos-group 5
Switch(config-pmap-c)#end
Switch#
```

## Related Commands

| Command | Description |
|---|---|
| match (class-map configuration) | Defines the match criteria for a class map. |
| policy-map | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| service-policy (policy-map class) | Creates a service policy that is a quality of service (QoS) policy within a policy map. |
| show policy-map | Displays information about the policy map. |
| show policy-map interface | Displays the statistics and configurations of the input and output policies that are attached to an interface. |

# shape (class-based queueing)

To enable traffic shaping a class of traffic in a policy map attached to a physical port, use the **shape average** policy-map class command. Traffic shaping limits the data transmission rate. To return to the default setting, use the **no** form of this command.

**shape average** {*rate*} [**bps** | **kbps** | **mbps** | **gbps**]

**shape average percent** {*percent_value*}

**no shape average**

## Syntax Description

| | |
|---|---|
| *rate* | Specifies an average rate for traffic shaping; the range is 16000 to 10000000000. Post-fix notation (k, m, and g) is optional and a decimal point is allowed. |
| **bps** | (Optional) Specifies a rate in bits per seconds. |
| **kbps** | (Optional) Specifies a rate in kilobytes per seconds. |
| **mbps** | (Optional) Specifies a rate in megabits per seconds. |
| **gbps** | (Optional) Specifies a rate in gigabits per seconds. |
| **percent** | Specifies a percentage of bandwidth for traffic shaping. |
| *percent_value* | (Optional) Specifies a percentage of the bandwidth used for traffic shaping; valid values are from 1 to 100 percent. |

## Defaults

Average-rate traffic shaping is disabled.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(40)SG | This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E. |

## Usage Guidelines

Use the **shape** command only in a policy map attached to a physical port. This command is valid in policy maps at any level of the hierarchy.

Shaping is the process of delaying out-of-profile packets in queues so that they conform to a specified profile. Shaping is distinct from policing. Policing drops packets that exceed a configured threshold, but shaping buffers packets so that traffic remains within the threshold. Shaping offers greater smoothness in handling traffic than policing.

You cannot use the **bandwidth**, **dbl**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

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

## Examples

This example shows how to limit the specified traffic class to a data transmission rate of 256 kbps:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

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

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Creates a signaling class structure that can be referred to by its name. |
| **class** | Specifies the name of the class whose traffic policy you want to create or change. |
| **dbl** | Enables active queue management on a transmit queue used by a class of traffic. |
| **policy-map** | Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode. |
| **service-policy (policy-map class)** | Creates a service policy that is a quality of service (QoS) policy within a policy map. |
| **show policy-map** | Displays information about the policy map. |

# shape (interface configuration)

To specify traffic shaping on an interface, use the **shape** command. To remove traffic shaping, use the **no** form of this command

**shape** [**rate**] [**percent**]

**no shape** [**rate**] [**percent**]

## Syntax Description

| | |
|---|---|
| **rate** | (Optional) Specifies an average rate for traffic shaping; the range is 16000 to 1000000000. Post-fix notation (k, m, and g) is optional and a decimal point is allowed. |
| **percent** | (Optional) Specifies a percent of bandwidth for traffic shaping. |

## Defaults

Default is no traffic shaping.

## Command Modes

Interface transmit queue configuration mode

## Command History

| Release | Modification |
|---|---|
| 12.2(18)EW | Support for this command was introduced on the Catalyst 4500 series switch. |

## Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

Traffic shaping is available on all the ports, and it sets an upper limit on the bandwidth.

When the high shape rates are configured on the Catalyst 4500 Supervisor Engine II-Plus-10GE (WS-X4013+10GE), the Catalyst 4500 Supervisor Engine V (WS-X4516), and the Catalyst 4500 Supervisor Engine V-10GE (WS-X4516-10GE), the shaped traffic rate may not be achieved in situations that involve contention and unusual packet size distributions. On the ports that are multiplexed through a Stub ASIC and connected to the backplane gigaports, the shape rates above 7 Mbps may not be achieved under worst-case conditions. On ports that are connected directly to the backplane gigaports, or the supervisor engine gigaports, the shape rates above 50 Mbps may not be achieved under worst-case conditions.

Some examples of ports that are connected directly to the backplane are as follows:

- Uplink ports on Supervisor Engine II+, II+10GE, III, IV, V, and V-10GE
- Ports on the WS-X4306-GB module
- The two 1000BASE-X ports on the WS-X4232-GB-RJ module
- The first two ports on the WS-X4418-GB module
- The two 1000BASE-X ports on the WS-X4412-2GB-TX module

All ports on the 24-port modules and the 48-port modules are multiplexed through a Stub ASIC. Some examples of ports multiplexed through a Stub ASIC are as follows:

- 10/100 ports on the WS-X4148-RJ45 module
- 10/100/1000 ports on the WS-X4124-GB-RJ45 module
- 10/100/1000 ports on the WS-X4448-GB-RJ45 module

## Examples

This example shows how to configure a maximum bandwidth (70 percent) for the interface fa3/1:

```
Switch(config)# interface fastethernet3/1
Switch(config-if)# tx-queue 3
Switch(config-if-tx-queue)# shape 70m
Switch(config-if-tx-queue)#
```