# 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 2-7 for valid values. |
| *number* | Module and port number. |

## Defaults

No interface types are configured.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Table 2-7 lists the valid values for *type*.

***Table 2-7 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 II 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 II only. |
| **atm** | ATM interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine II 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**. |
| **tunnel** | Tunnel interface. |

## 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)#
```

## Related Commands

show interfaces

# 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

## 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

**channel-group**
**show etherchannel**

# 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

Interface configuration

## 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

**define interface-range**
**show running config** (refer to Cisco IOS documentation)

# 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

## 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

arp access-list
show ip arp inspection

# 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

**show ip arp inspection**

# 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**

arp access-list
show ip arp inspection

# 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)
 ---------------  -----------     ----------
 Fa6/3            Trusted              None
Switch#
```

## Related Commands

**show ip arp inspection**

# 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 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 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

arp access-list
show arp access-list

# 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(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#
```

## Related Commands

**arp access-list**
**show ip arp inspection**

# 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

**arp access-list**
**show ip arp inspection**

# 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

## 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** show ip cef vlan

# 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

## 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

**ip dhcp snooping information option**
**ip dhcp snooping limit rate**
**ip dhcp snooping trust**
**ip dhcp snooping vlan**
**show ip dhcp snooping**
**show ip dhcp snooping binding**

# 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

## 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

**ip dhcp snooping**
**ip dhcp snooping information option**
**ip dhcp snooping trust**
**ip dhcp snooping vlan**
**show ip dhcp snooping**
**show ip dhcp snooping binding**

# 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

## 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

**ip dhcp snooping**
**ip dhcp snooping binding**
**ip dhcp snooping information option**
**ip dhcp snooping trust**
**ip dhcp snooping vlan**
**show ip dhcp snooping**
**show ip dhcp snooping binding**

# 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**

**no ip dhcp snooping information option**

## Syntax Description

This command has no arguments or keywords.

## Defaults

DHCP option 82 data insertion is enabled.

## Command Modes

Global configuration

## Command History

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

## 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)#
```

## Related Commands

**ip dhcp snooping**
**ip dhcp snooping limit rate**
**ip dhcp snooping trust**
**ip dhcp snooping vlan**
**show ip dhcp snooping**
**show ip dhcp snooping binding**

# 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

## 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

**ip dhcp snooping**
**ip dhcp snooping limit rate**
**ip dhcp snooping trust**
**ip dhcp snooping vlan**
**ip dhcp snooping information option**
**show ip dhcp snooping**
**show ip dhcp snooping binding**

# 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

## 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

**ip dhcp snooping**
**ip dhcp snooping information option**
**ip dhcp snooping trust**
**ip dhcp snooping vlan**
**show ip dhcp snooping**
**show ip dhcp snooping binding**

# 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

## 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

**ip dhcp snooping**
**ip dhcp snooping information option**
**ip dhcp snooping limit rate**
**ip dhcp snooping vlan**
**show ip dhcp snooping**
**show ip dhcp snooping binding**

# 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

## 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 the 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**

ip dhcp snooping
ip dhcp snooping information option
ip dhcp snooping limit rate
ip dhcp snooping trust
show ip dhcp snooping
show ip dhcp snooping binding

# 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

## 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

**ip igmp profile**
**show ip 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

## 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

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

**ip igmp filter**
**show ip 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

## 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** **ip igmp query-timeout** (refer to Cisco IOS documentation)
**ip pim query-interval** (refer to Cisco IOS documentation)
**show ip igmp groups** (refer to Cisco IOS documentation)

# 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

Interface configuration

## 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

**ip igmp snooping vlan immediate-leave**
**ip igmp snooping vlan mrouter**
**ip igmp snooping vlan static**

# 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

## 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**

ip igmp snooping vlan immediate-leave
ip igmp snooping vlan mrouter
ip igmp snooping vlan static

# 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

## 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

Before you can enable IGMP snooping on the Catalyst 4006 switches, you must configure the VLAN interface for multicast routing.

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

**ip igmp snooping vlan immediate-leave**
**ip igmp snooping vlan mrouter**
**ip igmp snooping vlan static**

# 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

**show ip igmp snooping membership**
**clear ip igmp snooping statistics vlan** (refer to Cisco IOS documentation)
**show ip igmp snooping statistics vlan** (refer to Cisco IOS documentation)

# 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

## 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

**ip igmp snooping**
**ip igmp snooping vlan mrouter**
**ip igmp snooping vlan static**
**show ip igmp interface** (refer to Cisco IOS documentation)
**show mac-address-table multicast**

# 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

## 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

**ip igmp snooping**
**ip igmp snooping vlan immediate-leave**
**ip igmp snooping vlan static**
**show ip igmp snooping**
**show ip igmp snooping mrouter**

# 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

## 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

**ip igmp snooping**
**ip igmp snooping vlan immediate-leave**
**ip igmp snooping vlan mrouter**
**show mac-address-table multicast**

# 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

## 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

**clear ip mfib fastdrop**
**show ip mfib fastdrop**

# 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 a per-interface basis.

# 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

## Command History

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

## 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

**show ip source binding**

# 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

## 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** **arp** (refer to Cisco IOS documentation)
**show arp** (refer to Cisco IOS documentation)

# 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 vlan dhcp-snooping

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

**ip verify source vlan dhcp-snooping** [**port-security**]

**no ip verify source vlan dhcp-snooping** [**port-security**]

## Syntax Description

| | |
|---|---|
| **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

## Command History

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

## Usage Guidelines

Interface configuration

## Examples

This example shows how to enable DHCP snooping security on VLANs 10 through 20:

```
Switch# config 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)# configure interface fastethernet6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport access vlan 10
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip dhcp snooping security interface fastethernet6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/1      ip           active       10.0.0.2                         10
fa6/1      ip           active       deny-all                         11-20
Switch#
```

The output shows that there is one valid DHCP binding to VLAN 10.

**Related Commands**

**debug ip verify source packet** (refer to Cisco IOS documentation)
**ip dhcp snooping**
**ip dhcp snooping limit rate**
**ip dhcp snooping information option**
**ip dhcp snooping trust**
**ip source binding** (refer to Cisco IOS documentation)
**show ip dhcp snooping**
**show ip dhcp snooping binding**
**show ip verify source** (refer to Cisco IOS documentation)
**show ip source binding** (refer to Cisco IOS documentation)

# 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 no Layer 2 protocol packets are tunneled.

## Command Modes

Interface configuration

## 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

**l2protocol-tunnel cos**
**l2protocol-tunnel drop-threshold**
**l2protocol-tunnel shutdown-threshold**

# 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

## 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

**l2protocol-tunnel**
**l2protocol-tunnel drop-threshold**
**l2protocol-tunnel shutdown-threshold**

# 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

## 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**

l2protocol-tunnel
l2protocol-tunnel cos
l2protocol-tunnel shutdown-threshold

# 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

## 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**

l2protocol-tunnel
l2protocol-tunnel cos
l2protocol-tunnel shutdown-threshold

# 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

**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**

**channel-group**
**channel-protocol**
**lacp system-priority**
**show lacp**

# 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

**channel-group**
**channel-protocol**
**lacp port-priority**
**show lacp**

# 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

## 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 2-8 describes the syntax of the **mac access-list extended** subcommands.

***Table 2-8 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: *source-mac-address source-mac-address-mask*. |
| **any** | Specifies any protocol type. |

*Table 2-8 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 2-9 lists which packets are mapped to a particular protocol family. |

Table 2-9 describes mapping an Ethernet packet to a protocol family.

*Table 2-9 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
```

**Related Commands** show vlan access-map

# 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

## 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

**show mac-address-table aging-time**

# 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

## 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#
```

**Related Commands** **mac-address-table dynamic** (refer to Cisco IOS documentation)

# 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

## 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)#
```

This example shows how to configure a static MAC address with IGMP snooping disabled for a specified address:

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

**Related Commands** show mac-address-table static

# 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

## 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**

macro apply cisco-phone
macro apply cisco-router
macro apply cisco-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

## 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

**macro apply cisco-desktop**
**macro apply cisco-router**
**macro apply cisco-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

## 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**

**macro apply cisco-desktop**
**macro apply cisco-phone**
**macro apply cisco-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

## 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**

macro apply cisco-desktop
macro apply cisco-phone
macro apply cisco-router

# 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

**auto-sync**

# 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

**show vlan access-map**
**vlan access-map**

# match flow ip

To specify match criteria to treat flows with a unique source or destination address as a new flow, use the **match flow ip** command. To disable this function, use the **no** form of this command.

**match flow ip** {**source-address** | **destination-address**}

**no match flow ip** {**source-address** | **destination-address**}

## Syntax Description

| | |
|---|---|
| **source-address** | Establishes a new flow from a flow with a unique IP source address. |
| **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 |

## 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 byte:

```
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#
```

Assume there are 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 byte:

```
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#
```

## Related Commands

**service-policy**
**show class-map**
**show policy-map**
**show policy-map interfaces** (refer to Cisco IOS documentation)

# 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

## 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 Release 12.2(18)EW, as well as Release 12.1(*xx*)E.

**Note** If you are upgrading the current supervisor engine from Release 12.2(18)EW or an earlier release to Release 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 II.

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

**redundancy**
**redundancy force-switchover**
**show redundancy**
**show running-config**

# 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*]} [ **,** | **-** | **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*]} [ **,** | **-** | **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 32, or by the following names: all, control-packet, rpf-failure, adj-same-if, nfl, mtu-exceeded, unknown-sa, span, acl input, acl input log, acl input error, acl input forward, acl input punt, acl output, acl output log, acl output error, acl output forward, acl output punt, bridged, bridged 1, bridged 2, bridged 3, bridged 4, routed received, routed received 1, routed received 2, routed received 3, routed received 4, routed forward, routed forward 1, routed forward 2, routed forward 3, and routed forward 4. |
| **,** | (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

## 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. |

## 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(config)# monitor session 1 filter ip access-group 100
Switch(config)#
```

This example shows how to add a source interface to a SPAN session:

```
Switch(config)# monitor session 1 source interface fa2/3
Switch(config)#
```

This example shows how to configure the sources with different directions within a SPAN session:

```
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)#
```

This example shows how to remove a source interface from a SPAN session:

```
Switch(config)# no monitor session 1 source interface fa2/3
Switch(config)#
```

This example shows how to limit SPAN traffic to VLANs 100 through 304:

```
Switch(config)# monitor session 1 filter vlan 100 - 304
Switch(config)#
```

This example shows how to configure RSPAN VLAN 20 as the destination:

```
Switch(config)# monitor session 2 destination remote vlan 20
Switch(config)#
```

## Related Commands

**show monitor**

# 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

**system mtu**

# 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

**instance**
**revision**
**show spanning-tree mst**
**spanning-tree mst configuration**

# 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

## 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 port channel address learning:

```
Switch(config-if)# pagp learn-method
Switch(config-if)#
```

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

**pagp learn-method**
**show pagp**

# 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

## 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

**pagp learn-method**
**show pagp**

# 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

**arp access-list**
**deny**
**ip arp inspection filter vlan**

# policy-map

To access the QoS policy map configuration mode to configure the QoS policy map, use the **policy-map** command. To delete a policy map, use the **no** form of this command.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

## Syntax Description

| | |
|---|---|
| *policy-map-name* | Specifies the name of the policy map. |

## Defaults

This command has no default settings.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

In QoS policy-map configuration mode, these configuration commands are available:

- **exit** exits QoS class map configuration mode.
- **no** removes an existing defined policy map.
- **class** *class-map-name* accesses the QoS class map configuration mode to specify a previously created class map to be included in the policy map or to create a class map. (See the **class-map** command for additional information.)
- **police** [**aggregate** *name*] *rate burst* [**conform-action** {**drop** | **transmit**}] [{**exceed-action** {**drop** | **policed-dscp-transmit** | **transmit**}}] defines a microflow or aggregate policer.
- **trust** {**cos** | **dscp**} sets the specified class trust values. Trust values that are set in this command supersede trust values that are set on specific interfaces.

## Examples

This example shows how to create a policy map named **ipp5-policy** that uses the class-map named **ipp5** and is configured to rewrite the packet precedence to 6 and to aggregate police the traffic that matches the IP precedence value of 5:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map ipp5-policy
Switch(config-pmap)# class ipp5
Switch(config-pmap-c)# set ip precedence 6
Switch(config-pmap-c)# police 2000000000 2000000 conform-action transmit exceed-action
policed-dscp-transmit
Switch(config-pmap-c)# end
```

**Related Commands**

class-map
service-policy
show class-map
show policy-map
show policy-map interface

# 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

## 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** interface port-channel
show etherchannel

# 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

## 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

**show power**

# 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) Maximum power that the equipment can consume; valid range is from 2000 to 15400 mW. |
| **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. 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.
- Default allocation is set to 15400.

## Command Modes

Interface configuration

## 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. |

## 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#
```

## Related Commands

**power inline consumption**
**show power**

# 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

## 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

**power inline**
**show power**

# 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

## 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 2-10 lists the maximum available power for chassis and Power over Ethernet for each power supply.

*Table 2-10 Available Power*

| Power Supply | Redundant Mode (W) | Combined Mode (W) |
|---|---|---|
| 1000 W AC | System[1] = 1000<br>Inline = 0 | System = 1667<br>Inline = 0 |
| 2800 W AC | System = 1360<br>Inline = 1400 | System = 2473<br>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

show power

# 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 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 mac-address 1.1.1
Switch(config-if-vlan-range)# exit
Switch#
```

## Related Commands

**port-security mac-address sticky**
**port-security maximum**

# 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.

## 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 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 mac-address sticky 1.1.1
Switch(config-if-vlan-range)# exit
Switch#
```

## Related Commands

**port-security mac-address**
**port-security maximum**

# 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

**port-security mac-address**
**port-security mac-address sticky**

# power supplies required

To configure the power redundancy mode for the Catalyst 4006 (only), use the **power supplies required** command. To return to the default power redundancy mode, use the **default** form of this command or the **power supplies required 2** command.

**power supplies required** {**1** | **2**}

**default power supplies required**

## Syntax Description

| | |
|---|---|
| **1** | Configures the chassis for 1+1 redundancy mode. |
| **2** | Configures the switch to 2+1 redundancy mode. |

## Defaults

2+1 redundancy mode

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(11)EW | Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4006 only). |

## Usage Guidelines

This command is not supported on a Catalyst 4500 series switch.

## Examples

This example shows how to set the power supplies that are required for the chassis to 1:

```
Switch(config)# power supplies required 1
Switch(config)#
```

## Related Commands

**show power**

# 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

## 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 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 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 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)#
```

## Related Commands

**show vlan**
**show vlan private-vlan**

# 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

## 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)#
```

## Related Commands

**show interfaces private-vlan mapping**
**show vlan**
**show vlan private-vlan**

# 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

**show spanning-tree mst**

# 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

## Command History

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

## Usage Guidelines

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

**qos (interface configuration mode)**
**show qos**

# 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

## Command History

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

## Usage Guidelines

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

**show qos**
**qos (global configuration mode)**

# 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

By default, 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 is included.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

In the Catalyst 4500 series switch, 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.

**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)#
```

This example shows how to disable the consistent accounting of the Layer 2 encapsulation by the QoS features:

```
Switch# config terminal
Switch(conf)# no qos account layer2 encapsulation
Switch (conf)#
```

**Related Commands**

**show interfaces**
**switchport**
**switchport block**

# 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

## Command History

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

## Usage Guidelines

This policer can be shared by different policy map classes and on different interfaces.

The Catalyst 4006 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 2-11 are allowed.

*Table 2-11 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 2-12 are allowed.

*Table 2-12 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

show qos aggregate policer

# 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

The default CoS value is 0.

**Note** CoS override is not configured.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

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

**show qos**

# 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*} | **exceed-action** {**ecn** | **probability** *percent*} | **flow** {**include** [**layer4-ports**] [**vlan**]}]

**no qos dbl** [**buffers** {**aggressive-flow** *buffers*} | **credits** {**aggressive-flow** *credits* | **maximum** *max*} | **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. |
| **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

The default settings are as follows:

- QoS DBL is disabled.
- Aggressive-flow buffers is set to 2.
- Aggressive-flow credits is set to 2.
- Layer 4 ports are included.
- VLANs are included.
- 15 maximum credits are allowed.
- 15% drop probability is set.

## Command Modes

Global configuration

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. |

## 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 p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)#
```

## Related Commands

**show qos dbl**

# 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

The default DSCP value is 0.

## Command Modes

Interface configuration

## 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 configure the default QoS DSCP value as 6:

```
Switch(config-if)# qos dscp 6
Switch(config-if)#
```

## Related Commands

**show qos 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 clear the entire mapping table, 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

## Command History

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

## Usage Guidelines

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 value. 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**

qos map dscp
qos map dscp policed
show qos

# 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

## Command History

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

## Usage Guidelines

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

qos map cos
show qos interface
show qos
tx-queue

# 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

## Command History

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

## Usage Guidelines

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

**qos map cos**
**qos map dscp**
**show qos**

# 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

## Command History

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

## Usage Guidelines

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

**qos (global configuration mode)**
**show qos**

# 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

## 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

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

**qos cos**
**qos vlan-based**
**show qos 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

## Command History

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

## Usage Guidelines

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

**qos cos**
**show qos interface**

# 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

## 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-r)#
```

This example shows how to enter the main CPU submode:

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)#
```

## Related Commands

**auto-sync**
**main-cpu**

# 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

**redundancy**
**show redundancy**

# 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

**redundancy**
**show redundancy**

# 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 4006 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

**attach module**
**session module**

# 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

## 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

monitor session

# 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

## 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

**ip dhcp snooping**
**ip dhcp snooping binding**
**ip dhcp snooping information option**
**ip dhcp snooping trust**
**ip dhcp snooping vlan**
**show ip dhcp snooping**
**show ip dhcp snooping binding**

# 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

## 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

**instance**
**name**
**show spanning-tree mst**
**spanning-tree mst configuration**

# service-policy

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.

## Command Modes

Interface configuration

## 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.

You cannot apply a policy-map under an interface and a VLAN range at the same time.

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

## Related Commands

**class-map**
**policy-map**
**service-policy**
**show policy-map interface vlan**

# session module

To remotely connect to a specific module, 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 |
|---|---|
| 12.1(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 that is used. For example, if you have a Catalyst 4006 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 **session module** *mod* command, the prompt changes to Gateway#.

The session command is identical to the **attach module** *mod* and the **remote login module** *mod* commands.

## Examples

This example shows how to remotely log in to the Access Gateway Module:

```
Switch# session module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

## Related Commands

**attach module**
**remote login module**

# shape

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

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 V (WS-X4516), 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+, III, IV, and V
- 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)#
```