eigrp event-log-size

To set the size of the IP-EIGRP event log, use the **eigrp event-log-size** command.

eigrp event-log-size *size*

Syntax Description

size	IP-EIGRP event log size; valid values are from 0 to 4294967295.

Command Default

This command has no default settings.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Once the configured event log size has been exceeded, the last configured (event-log-size) number of lines of log is retained.

Examples

This example shows how to set the size of the IP-EIGRP event log:

```
Router (config-router)# eigrp event-log-size 5000010
Router (config-router)#
```

Related Commands

Command	Description
clear ip eigrp event	Clears the IP-EIGRP event log.

encapsulation dot1q

To enable the IEEE 802.1Q encapsulation of traffic on a specified subinterface in the VLANs, use the **encapsulation dot1q** command.

encapsulation dot1q *vlan-id* [**native**]

Syntax Description

vlan-id	Virtual LAN identifier; valid values are from 1 to 4094.
native	(Optional) Sets the PVID value of the port to the *vlan-id* value.

Command Default

This command has no default settings.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Always use the **native** keyword when the *vlan-id* is the ID of the 802.1Q native VLAN. Do not configure encapsulation on the native VLAN of an 802.1Q trunk without the **native** keyword.

To enter the subinterface configuration mode, you must enter the interface configuration mode first and then enter the **interface** command to specify a subinterface.

Examples

This example shows how to set encapsulation for VLAN traffic using the 802.1Q protocol for VLAN 100:

```
Router(config-subif)# encapsulation dot1q 100
Router(config-subif)#
```

Related Commands

Command	Description
encapsulation isl	Enables ISL.

encapsulation isl

To enable ISL, use the **encapsulation isl** command.

encapsulation isl *vlan-identifier*

Syntax Description

vlan-identifier	VLAN identifier; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

ISL is a Cisco protocol that is used for interconnecting multiple switches and routers and for defining VLAN topologies.

ISL encapsulation adds a 26-byte header to the beginning of the Ethernet frame. The header contains a 10-bit VLAN identifier that conveys VLAN membership identities between the switches.

To enter the subinterface configuration mode, you must enter the interface configuration mode first and then enter the **interface** command to specify a subinterface.

Examples

This example shows how to enable ISL on Fast Ethernet subinterface 2/1.20:

```
Router(config-subif)# encapsulation isl 400
Router(config-subif)#
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
show bridge vlan	Displays virtual LAN subinterfaces.
show interfaces	Displays the traffic that is seen by a specific interface.
show vlans	Displays information about the Cisco IOS VLAN subinterfaces.

erase

To erase a file system, use the **erase** command.

erase {**const_nvram:** | **nvram:** | **startup-config:**}

Syntax Description

const_nvram:	Erases all files under the const_nvram: partition.
nvram:	Erases NVRAM.
startup-config:	Erases the contents of the configuration memory.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Caution When you use the **erase** command to erase a file system, you cannot recover the files in the file system.

The **erase nvram:** command replaces the **write erase** command and the **erase startup-config** command.

You can use the **erase** command on both Class B and Class C flash file systems only. To reclaim space on flash file systems after deleting files using the **delete** command, you must use the **erase** command. The **erase** command erases all of the files in the flash file system.

Class A flash file systems cannot be erased. You can delete individual files using the **delete** command and then reclaim the space using the **squeeze** command. You can also use the **format** command to format the flash file system.

On Class C flash file systems, space is dynamically reclaimed when you use the **delete** command. You can also use either the **format** or **erase** command to reinitialize a Class C flash file system.

The **erase nvram:** command erases NVRAM. On Class A file system platforms, if the CONFIG_FILE variable specifies a file in flash memory, the specified file is marked "deleted."

You can enter the **erase const_nvram** command to erase the VLAN database configuration file.

Examples

This example shows how to erase the NVRAM and the startup configuration in the NVRAM:

```
Router# erase nvram:
Router#
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the system configures itself during initialization (startup).
delete	Deletes a file from a flash memory device or NVRAM.
more nvram:startup-config:	Displays the startup configuration file contained in NVRAM or specified by the CONFIG-FILE environment variable.
show bootvar	Displays information about the BOOT environment variable.
undelete	Recovers a file that is marked “deleted” on a flash file system.

errdisable detect cause

To enable the error-disable detection, use the **errdisable detect cause** command. To disable the error-disable detection, use the **no** form of this command.

errdisable detect cause {**all** | **dtp-flap** | **l2ptguard** | **link-flap** | **packet-buffer-error** | **pagp-flap** | **udld**}

no errdisable detect cause {**all** | **dtp-flap** | **l2ptguard** | **link-flap** | **pagp-flap** | **udld**}

Syntax Description

all	Specifies error-disable detection for all error-disable causes.
dtp-flap	Specifies detection for the DTP flap error-disable cause.
l2ptguard	Specifies detection for the Layer 2 protocol-tunnel error-disable cause.
link-flap	Specifies detection for the link flap error-disable cause.
packet-buffer-error	Causes the packet buffer error to error-disable the affected port.
pagp-flap	Specifies detection for the PAgP flap error-disable cause.
udld	Specifies detection for the UDLD error-disable cause.

Command Default

Enabled for all causes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Note Entering the **no errdisable detect cause packet-buffer-error** command allows you to detect the fault that triggers a power cycle of the affected module.

A cause (bpduguard, dtp-flap, link-flap, pagp-flap, root-guard, udld) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state (an operational state that is similiar to the link-down state).

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

Examples

This example shows how to enable the error-disable detection for the Layer 2 protocol-tunnel guard error-disable cause:

```
Router(config)# errdisable detect cause l2ptguard
Router(config)#
```

Related Commands

Command	Description
show errdisable detect	Displays the error-disable detection status.
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

errdisable recovery

To configure the recovery mechanism variables, use the **errdisable recovery** command. To return to the default state, use the **no** form of this command.

errdisable recovery cause {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **udld** | **unicast-flood**}

errdisable recovery {**interval** *interval*}

no errdisable recovery cause {**all** | {**arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **udld** | **unicast-flood**}

no errdisable recovery {**interval** *interval*}

Syntax Description

cause	Enables error-disable recovery to recover from a specific cause.
all	Enables the recovery timers for all error-disable causes.
arp-inspection	Enables error-disable recovery to recover from an ARP inspection cause.
bpduguard	Enables the recovery timer for the BPDU-guard error-disable cause.
channel-misconfig	Enables the recovery timer for the channel-misconfig error-disable cause.
dhcp-rate-limit	Enables the recovery timer for the DHCP rate-limit error-disable cause.
dtp-flap	Enables the recovery timer for the DTP-flap error-disable cause.
gbic-invalid	Enables the recovery timer for the GBIC invalid error-disable cause.
l2ptguard	Enables the recovery timer for the Layer 2 protocol-tunnel error-disable cause.
link-flap	Enables the recovery timer for the link-flap error-disable cause.
pagp-flap	Enables the recovery timer for the PAgP-flap error-disable cause.
pesecure-violation	Enables the recovery timer for the pesecure-violation error-disable cause.
security-violation	Enables the automatic recovery of ports that were disabled due to 802.1X security violations.
udld	Enables the recovery timer for the UDLD error-disable cause.
unicast-flood	Enables the recovery timer for the unicast-flood error-disable cause.
interval *interval*	Specifies the time to recover from a specified error-disable cause; valid values are from 30 to 86400 seconds.

Command Default

The defaults are as follows:

- Disabled for all causes.
- If enabled, the *interval* is 300 seconds.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **secure-violation** option is not supported.

A cause (bpduguard, dhcp-rate-limit, dtp-flap, l2ptguard, link-flap, pagp-flap, security-violation, channel-misconfig, psecure-violation, udld, or unicast-flood) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state (an operational state that is similiar to the link-down state). If you do not enable errdisable recovery for the cause, the interface stays in the error-disabled state until a shutdown and no shutdown occurs. If you enable recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry operation once all the causes have timed out.

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

Examples

This example shows how to enable the recovery timer for the BPDU-guard error-disable cause:

```
Router(config)# errdisable recovery cause bpduguard
Router(config)#
```

This example shows how to set the timer to 300 seconds:

```
Router(config)# errdisable recovery interval 300
Router(config)#
```

Related Commands

Command	Description
show errdisable recovery	Displays the information about the error-disable recovery timer.
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

error-detection packet-buffer action

To specify the action that a module takes after packet buffer memory failures, use the **error-detection packet-buffer action** command. To return to the default settings, use the **no** form of this command.

error-detection packet-buffer action {**module** *num*} {**error-disable** | **power-down** | **reset**}

Syntax Description

module *num*	Specifies the module number.
error-disable	Error disables the module.
power-down	Powers down the module.
reset	Resets the module.

Command Default

Error-disable port group

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on the following modules only:

- WS-X6348-RJ-45
- WS-X6348-RJ-21V
- WS-X6248-RJ-45
- WS-X6248-TEL
- WS-X6148-RJ-45
- WS-X6148-RJ-21

When you specify the **reset** keyword, a rapid reboot (approximately 10 seconds) and not a normal reboot (approximately 45 to 50 seconds) is performed. Prior to this release, the module always went through a non-rapid reboot.

Examples

This example shows how to set the module to error disable after packet buffer memory failures:

```
Router(config)# error-detection packet-buffer action module 2 error-disable
Router(config)#
```

This example shows how to set the module to power down after packet buffer memory failures:

```
Router(config)# error-detection packet-buffer action module 2 power-down
Router(config)#
```

This example shows how to set the module to reset after packet buffer memory failures:

```
Router(config)# error-detection packet-buffer action module 2 reset
Router(config)#
```

file verify auto

To verify the compressed Cisco IOS image checksum, use the **file verify auto** command. To turn off automatic verification after a copy operation, use the **no** form of this command.

file verify auto

no file verify auto

Syntax Description

This command has no arguments or keywords.

Command Default

Verification is done automatically after completion of a copy operation.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Enter the **copy /noverify** command to override the default behavior for a single copy operation.

Examples

This example shows how to verify the compressed Cisco IOS image checksum:

```
Router(config)# file verify auto
Router(config)#
```

Related Commands

Command	Description
copy /noverify	Disables the automatic image verification for the current copy operation.
verify	Verifies the checksum of a file on a flash memory file system or computes an MD5 signature for a file.

flowcontrol

To configure a port to send or receive pause frames, use the **flowcontrol** command.

flowcontrol {**send** | **receive**} {**desired** | **off** | **on**}

Syntax Description

send	Specifies that a port sends pause frames.
receive	Specifies that a port processes pause frames.
desired	Obtains predictable results regardless of whether a remote port is set to **on**, **off**, or **desired**.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.

Command Default

Flow-control defaults depend upon port speed. The defaults are as follows:

- Gigabit Ethernet ports default to **off** for receive and **desired** for send.
- Fast Ethernet ports default to **off** for receive and **on** for send.
- On the 24-port 100BASE-FX and 48-port 10/100 BASE-TX RJ-45 modules, the default is **off** for receive and **off** for send.
- 10-Gigabit Ethernet ports are permanently configured to respond to pause frames, and the default for send is **off**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **send** and **desired** keywords are supported on Gigabit Ethernet ports only.

Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

Gigabit Ethernet ports on the Catalyst 6500 series switches use flow control to inhibit the transmission of packets to the port for a period of time; other Ethernet ports use flow control to respond to flow-control requests.

If a Gigabit Ethernet port receive buffer becomes full, the port transmits a “pause” packet that tells remote ports to delay sending more packets for a specified period of time. All Ethernet ports (1000 Mbps, 100 Mbps, and 10 Mbps) can receive and act upon “pause” packets from other devices.

You can configure non-Gigabit Ethernet ports to ignore received pause frames (**disable**) or to react to them (**enable**).

When used with **receive**, the **on** and **desired** keywords have the same result.

All Catalyst 6500 series switch Gigabit Ethernet ports can receive and process pause frames from remote devices.

To obtain predictable results, follow these guidelines:

- Use **send on** only when remote ports are set to **receive on** or **receive desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.
- Use **receive on** only when remote ports are set to **send on** or **send desired**.
- Use **send off** only when remote ports are set to **receive off** or **receive desired**.

Examples

These examples show how to configure the local port to not support any level of flow control by the remote port:

```
Router(config-if)# flowcontrol receive off
Router(config-if)#

Router(config-if)# flowcontrol send off
Router(config-if)#
```

Related Commands

Command	Description
show interfaces flowcontrol	Displays flow-control information.

format

To format a Class A or Class C flash file system, use the **format** command.

Class A flash file system:

format bootflash: [**spare** *spare-number*] *filesystem1***:** [[*filesystem2***:**][*monlib-filename*]]

Class C flash file system:

format *filesystem1***:**

Caution Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the flash PC card can still be used. Otherwise, you must reformat the flash PC card when some of the sectors fail.

Syntax Description

spare *spare-number*	(Optional) Specifies the number of the spare sectors to reserve on formatted flash memory; valid values are from 0 to 16.
*filesystem1***:**	File system to format; valid values are **disk0:**, **bootdisk:**, and **sup-bootdisk:**; see the "Usage Guidelines" section for additional information.
*filesystem2***:**	(Optional) File system containing the monlib file to use for formatting filesystem1 followed by a colon.
monlib-filename	(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the *filesystem1* argument.

Command Default

The defaults are as follows:

- *monlib-filename* is the one bundled with the system software.
- *spare-number* is zero (0).

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command to format Class A or C flash memory file systems.

The Supervisor Engine 32 PISA has these flash memory devices:

- **disk0:**
  - One external CompactFlash Type II slot
  - Supports CompactFlash Type II Flash PC cards
- **sup-bootdisk:**
  - Supervisor Engine 32 PISA 256-MB internal CompactFlash flash memory
  - From the Supervisor Engine 32 PISA ROMMON, it is bootdisk:
- **bootdisk:**
  - PISA 256-MB internal CompactFlash flash memory
  - Not accessible from the Supervisor Engine 32 PISA ROMMON

In some cases, you might need to insert a new flash PC card and load images or back up configuration files onto it. Before you can use a new flash PC card, you must format it.

Sectors in flash PC cards can fail. Reserve certain flash PC sectors as "spares" by using the optional *spare* argument on the **format** command to specify between 0 and 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the flash PC card. If you specify 0 spare sectors and some sectors fail, you must reformat the flash PC card, which erases all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the flash file system. The Cisco IOS system software contains a monlib file.

When used with HSA and you do not specify the *monlib-filename* argument, the system takes the ROM monitor library file from the slave image bundle. If you specify the *monlib-filename* argument, the system assumes that the files reside on the slave devices.

In the command syntax, *filesystem1:* specifies the device to format, and *filesystem2:* specifies the optional device containing the monlib file, used to format *filesystem1:*. If you omit the optional *filesystem2:* and *monlib-filename* arguments, the system formats *filesystem1:,* using the monlib file that is already bundled with the system software. If you omit only the optional *filesystem2:* argument, the system formats *filesystem1:,* using the monlib file from the device that you specified with the **cd** command. If you omit only the optional *monlib-filename* argument, the system formats *filesystem1:* using *filesystem2:*'s monlib file. When you specify both arguments—*filesystem2:* and *monlib-filename*—the system formats *filesystem1:,* using the monlib file from the specified device. You can specify *filesystem1:*'s own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.

Examples

This example shows how to format a CompactFlash PC card that is inserted in slot 0:

```
Router# format disk0:
Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device disk0 completed
```

When the console returns to the EXEC prompt, the new CompactFlash PC card is successfully formatted and ready for use.

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
delete	Deletes a file from a flash memory device or NVRAM.
show file systems	Lists available file systems.
undelete	Recovers a file that is marked as "deleted" on a flash file system.

fsck

To check a flash file system for damage and to repair any problems, use the **fsck** command.

fsck [**/automatic** | **disk0:**]

Syntax Description

/automatic	(Optional) Specifies automatic mode; see the "Usage Guidelines" section for additional information.
disk0:	(Optional) Specifies the file system to check.

Command Default

The current file system is checked if **disk0:** is not specified.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is valid only on Class C flash file systems and on PCMCIA ATA flash disks and CompactFlash disks.

If you do not enter any arguments, the current file system is used. Use the **pwd** command to display the current file system.

If you enter the **disk0:** keyword, the fsck utility checks the selected file system for problems. If a problem is detected, a prompt is displayed asking if you want the problem fixed.

If you enter the **/automatic** keyword, you are prompted to confirm that you want the automatic mode. In automatic mode, problems are fixed automatically and you are not prompted to confirm.

Table 2-9 lists the checks and actions that are performed by the fsck utility.

Table 2-9 fsck Utility Checks and Actions

Checks	Actions
Checks the boot sector and the partition table and reports the errors.	No action.
Validates the media with the signature in the last 2 bytes of the first sector (0x55 and 0xaa, respectively).	No action.
Checks the os_id to find whether this is a FAT-12 or FAT-16 file system (valid values include 0, 1, 4, and 6).	No action.
Checks the number of FAT's field (correct values are 1 and 2).	No action.

Table 2-9 fsck Utility Checks and Actions (continued)

Checks	Actions
Checks these values: - n_fat_sectors cannot be less than 1. - n_root_entries cannot be less than 16. - n_root_sectors cannot be less than 2. - base_fat_sector, n_sectors_per_cluster, n_heads, n_sectors_per_track is not 0.	No action.
Checks the files and FAT for these errors:	
Checks the FAT for invalid cluster numbers.	If the cluster is a part of a file chain, the cluster is changed to end of file (EOF). If the cluster is not part of a file chain, it is added to the free list and unused cluster chain. Table 2-10 lists valid cluster numbers; numbers other than those listed in Table 2-10 are invalid numbers.
Checks the file's cluster chain for loops.	If the loop is broken, the file is truncated at the cluster where the looping occurred.
Checks the directories for nonzero size fields.	If directories are found with nonzero size fields, the size is reset to zero.
Checks for invalid start cluster file numbers.	If the start cluster number of a file is invalid, the file is deleted.
Checks files for bad or free clusters.	If the file contains bad or free clusters, the file is truncated at the last good cluster; an example is the cluster that points to this bad/free cluster.
Checks to see if the file's cluster chain is longer than indicated by the size fields.	If the file's cluster chain is longer than indicated by the size fields, the file size is recalculated and the directory entry is updated.
Checks to see if two or more files share the same cluster (crosslinked).	If two or more files are crosslinked, you are prompted to accept the repair, and one of the files is truncated.
Checks to see if the file's cluster chain is shorter than is indicated by the size fields.	If the file's cluster chain is shorter than is indicated by the size fields, the file size is recalculated and the directory entry is updated.
Checks to see if there are any unused cluster chains.	If unused cluster chains are found, new files are created and linked to that file with the name fsck-*start cluster*.

Table 2-10 Valid Cluster Numbers

Cluster	FAT-12	FAT-16
Next entry in the chain	2-FEF	2-FFEF
Last entry in chain	FF8-FFF	FFF8-FFFF
Available cluster	0	0
Bad cluster	FF7	FFF7

Examples

This example shows how to run a check of the current file system:

```
Router# fsck
 Checking the boot sector and partition table...
 Checking FAT, Files and Directories...
 Files
 1) disk0:/FILE3 and
 2) disk0:/FILE2
 have a common cluster.
 Press 1/2 to truncate or any other character to ignore[confirm] q
 Ignoring this error and continuing with the rest of the check...
 Files
 1) disk0:/FILE5 and
 2) disk0:/FILE4
 have a common cluster.
 Press 1/2 to truncate or any other character to ignore[confirm] 1
 File disk0:/FILE5 truncated.
 Files
 1) disk0:/FILE7 and
 2) disk0:/FILE6
 have a common cluster.
.
.
.
1) disk0:/FILE15 and
 2) disk0:/FILE13
 have a common cluster.
 Press 1/2 to truncate or any other character to ignore[confirm] i
 Ignoring this error and continuing with the rest of the check...
 Reclaiming unused space...
 Created file disk0:/fsck-11 for an unused cluster chain
 Created file disk0:/fsck-20 for an unused cluster chain
 Created file disk0:/fsck-30 for an unused cluster chain
 Created file disk0:/fsck-35 for an unused cluster chain
 Created file disk0:/fsck-40 for an unused cluster chain
 Created file disk0:/fsck-46 for an unused cluster chain
 Created file disk0:/fsck-55 for an unused cluster chain
 Created file disk0:/fsck-62 for an unused cluster chain
 Created file disk0:/fsck-90 for an unused cluster chain
 Updating FAT...
 fsck of disk0: complete
Router#
```

hold-queue

To limit the size of the IP output queue on an interface, use the **hold-queue** command. To return to the default settings, use the **no** form of this command.

hold-queue *length* {**in** | **out**}

no hold-queue {**in** | **out**}

Syntax Description

length	Maximum number of packets in the queue; valid values are from 0 to 65535.
in	Specifies the input queue.
out	Specifies the output queue.

Command Default

The defaults are as follows:

- The input hold-queue limit is 75 packets.
- The default output hold-queue limit is 40 packets.
- The default is 10 packets for asynchronous interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is not supported on the OSM.

The default limits prevent a malfunctioning interface from consuming an excessive amount of memory. There is no fixed upper limit to a queue size.

The default of ten packets allows the Cisco IOS software to queue a number of back-to-back routing updates. The default is for asynchronous interfaces only; other media types have different defaults.

The guidelines for hold queues and priority queueing are as follows:

- The hold queue stores packets that are received from the network and are waiting to be sent to the client. We recommend that the queue size does not exceed ten packets on asynchronous interfaces. For most other interfaces, the queue length should not exceed 100 packets.
- The input hold queue prevents a single interface from flooding the network server with too many input packets. Additional input packets are discarded if the interface has too many outstanding input packets in the system.
- If you use priority output queueing, you can set the length of the four output queues using the **priority-list** global configuration command.You cannot use the **hold-queue** command to set an output hold-queue length in this situation.
- For slow links, use a small output hold-queue limit to prevent storing packets at a rate that exceeds the transmission capability of the link.

- For fast links, use a large output hold-queue limit. A fast link may be busy for a short time (and require the hold queue) but can empty the output hold queue quickly when capacity returns.
- You can display the current hold-queue setting and the number of packets that are discarded because of hold-queue overflows by using the **show interfaces** command in EXEC mode.

Caution Increasing the hold queue can cause negative effects to network routing and response times. If you use protocols that have sequence/acknowledge packets to determine round-trip times, do not increase the output queue. Instead, we recommend that you program the Catalyst 6500 series switch to drop packets and inform the hosts to slow down transmissions to match the available bandwidth. We do not recommend that you make duplicate copies of the same packet within the network.

Examples

This example sets a small input queue on a slow serial line:

```
Router(config)# interface serial 0
Router(config-if)# hold-queue 30 i
```

Related Commands

Command	Description
priority-list	Establishes queueing priorities based on the protocol type.
show interfaces	Displays the traffic that is seen by a specific interface.

hw-module boot

To specify the boot options for the module through the power management bus control register, use the **hw-module boot** command.

hw-module {**module** *num*} {**boot** [*value*] {**config-register** | **eobc** | {**flash** *image*} | **rom-monitor**}}

Syntax Description

module *num*	Specifies the number of the module to apply the command.
value	(Optional) Literal value for the module's boot option; valid values are from 0 to 15. See the "Usage Guidelines" section for additional information.
config-register	Boots using the module's config-register value.
eobc	Boots using an image downloaded through EOBC.
flash *image*	Specifies the image number in the module's internal flash memory for the module's boot option; valid values are 1 and 2.
rom-monitor	Stays in ROM-monitor mode after the module resets.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on the CMM only.

The valid values for the **boot** *value* argument are as follows:

- 0—Specifies the module's config-register value.
- 1—Specifies the first image in the flash memory.
- 2—Specifies the second image in the flash memory.
- 3—Stays in ROM-monitor mode after the module reset.
- 4—Specifies the download image through EOBC.

Examples

This example shows how to reload the module in slot 6 using the module's config-register value:

```
Router# hw-module slot 1/6 boot config-register
Router#
```

This example shows how to reload the module in slot 3 using an image downloaded through EOBC:

```
Router# hw-module slot 1/3 boot eobc
Router#
```

hw-module fan-tray version

To set the fan-type (high or low power) version, use the **hw-module fan-tray version** command.

hw-module fan-tray version [**1** | **2**]

Syntax Description

1 | **2**	(Optional) Specifies the version number; see the "Usage Guidelines" section for additional information.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Before you install a high-capacity fan tray, enter the **hw-module fan-tray version 2** command to check for configuration problems, such as power-supply compatibility and power sufficiency. If there are no problems, a message is displayed to change the fan tray from version 1 to version 2. At this point, you can remove the old fan tray and quickly insert the new high-capacity fan tray.

This command is supported on the following chassis:

- WS-C6506
- WS-C6509
- WS-C6509-NEB/OSR7609

Set the version to **2** before installing higher power fan trays. Set the version to **1** before downgrading to lower power fan trays.

Command confirmation does not change the fan power consumption or cooling capacity. It updates the backplane IDPROM. The new values take effect the next time that you insert a fan.

When you execute the command, the software checks the configurations and prompts for confirmation. Any illegal configurations (such as power-supply incompatibility) result in a warning being displayed and a command failure.

Examples

This example shows how to set the fan type for lower power fan trays:

```
Router # hw-module fan-tray version 1
Router #
```

Related Commands

Command	Description
show environment cooling	Displays information about the cooling parameter.

hw-module oversubscription

To administratively disable the oversubscribed ports (3, 4, 7, and 8) on a module, use the **hw-module oversubscription** command. Use the **no** form of this command to enable the oversubscribed ports.

hw-module {**module** *num*} **oversubscription**

no hw-module {**module** *num*} **oversubscription**

Syntax Description

module *num*	Applies the command to a specific module.

Command Default

Enabled.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on the WS-X6708-10G-3C and the WS-X6708-10G-3CXL modules only.

When you disable the oversubscribed ports, the port is put into shutdown mode. In this mode, you cannot enter the **no shut** command on the disabled ports. If you attempt to enter the **no shut** command on the disabled ports, this message appears:

```
The current module is operating in non-oversubscription mode. To utilise this interface,
enable oversubscription mode for the module.
```

The *num* argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

When you enter the **show interfaces** command on the disabled ports, the output displays “disabled for performance” to distinguish between the normal port shutdown and the shutdown for performance.

Examples

This example shows how to administratively disable the oversubscribed ports on a module:

```
Router # hw-module module 3 oversubscription
Router #
```

This example shows how to administratively enable the oversubscribed ports on a module:

```
Router # no hw-module module 3 oversubscription
Router #
```

Related Commands

Command	Description
show interfaces	Displays traffic that is seen by a specific interface.

hw-module reset

To reset a module by turning the power off and then on, use the **hw-module reset** command.

hw-module {**module** *num*} **reset**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *num* argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples

This example shows how to reload a specific module:

```
Router # hw-module module 3 reset
Router #
```

hw-module shutdown

To shut down the module, use the **hw-module shutdown** command.

hw-module {**module** *num*} **shutdown**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on the SSL Services Module and the NAM.

If you enter the **hw-module shutdown** command to shut down the module, you will have to enter the **no power enable module** command and the **power enable module** command to restart (power down and then power up) the module.

Examples

This example shows how to shut down and restart the module:

```
Router# hw-module module 3 shutdown
Router# no power enable module 3
Router# power enable module 3
```

hw-module simulate link-up

To enable a software link on a specified module, use the **hw-module simulate link-up** command. For information on disabling a software link, refer to the "Usage Guidelines" section.

hw-module {**module** *num*} **simulate link-up**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on Ethernet modules only.

To disable a software link on a module, you must perform one of the following procedures:

- Enter the **shutdown** and then the **no shutdown** commands on all the ports on the module.
- Enter the **hw-module reset** command.

When you apply this command to a module, the port LEDs on the module will glow green and simulate a link-up condition. This command can be used for testing interface configurations without cabling to the interface.

The *num* argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples

This example shows how to enable softlink on a module:

```
Router# hw-module module 3 simulate link-up
Router#
```

Related Commands

Command	Description
hw-module reset	Resets a module by turning the power off and then on.

instance

To map a VLAN or a set of VLANs to an MST instance, use the **instance** command. To return the VLANs to the default instance (CIST), use the **no** form of this command.

instance *instance-id* {**vlans** *vlan-range*}

no instance *instance-id*

Syntax Description

instance-id	Instance to which the specified VLANs are mapped; valid values are from 0 to 4094.
vlans *vlan-range*	Specifies the number of the VLANs to be mapped to the specified instance; valid values are from 1 to 4094.

Command Default

No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

Command Modes

MST configuration submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **vlans** *vlan-range* is entered as a single value or a range.

The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing instances.

Any unmapped VLAN is mapped to the CIST instance.

You can configure up to 65 interfaces

Examples

This example shows how to map a range of VLANs to instance 2:

```
Router(config-mst)# instance 2 vlans 1-100
Router(config-mst)#
```

This example shows how to map a VLAN to instance 5:

```
Router(config-mst)# instance 5 vlans 1100
Router(config-mst)#
```

This example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Router(config-mst)# no instance 2 vlans 40-60
Router(config-mst)#
```

This example shows how to move all the VLANs that are mapped to instance 2 back to the CIST instance:

```
Router(config-mst)# no instance 2
Router(config-mst)#
```

Related Commands

Command	Description
name (MST configuration submode)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show	Verifies the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst configuration	Enters MST-configuration submode.

interface

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

interface {*type module*} [.*subinterface*]

Syntax Description

type	Type of interface to be configured; see Table 2-11 for valid values.
module	Module and port number or port-subinterface number; see the "Usage Guidelines" section for additional information.
.*subinterface*	(Optional) Subinterface number to be configured; valid values are from 0 to 4294967295.

Command Default

No interface types are configured.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Table 2-11 lists the valid values for *type*.

Table 2-11 Valid type Values

Keyword	Definition
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.
pos	Packet OC-3 interface on the Packet over SONET Interface Processor.
atm	ATM interface.
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.

By default, the Supervisor Engine 32 PISA EtherChannel (port channel interface 256, which is automatically configured with the **pisa-channel** command) is a 1-Gps EtherChannel.

Note The **pisa-channel** command is visible in the configuration file, but it is not user configurable.

You can enter the number of a port subinterface in the following format:

interface {{*type module/port.subinterface*}}

The Supervisor Engine 32 PISA ports are as follows:

- Supervisor Engine 32 PISA Management Ports—The console port for the Supervisor Engine 32 PISA port is an EIA/TIA-232 (RS-232) port. The Supervisor Engine 32 PISA also has two Universal Serial Bus (USB) 2.0 ports that currently are not enabled.
- Supervisor Engine 32 PISA Data Ports for the WS-S32-10GE-PISA has the following ports:
  - Ports 1 and 2: XENPAK 10 Gigabit Ethernet
  - Port 3: 10/100/1000 Mbps RJ-45

  Note You can disable Port 3 and reallocate its port ASIC capacity to the PISA EtherChannel (see the "Configuring Full PISA EtherChannel Bandwidth" section in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*}.

- Supervisor Engine 32 PISA Data Ports for the WS-S32-GE-PISA has these ports:
  - Ports 1 through 8: Small form-factor pluggable (SFP) Gigabit Ethernet
  - Port 9: 10/100/1000 Mbps RJ-45 port

  Note You can disable port 9 and reallocate its port ASIC capacity to the PISA EtherChannel (see the "Configuring Full PISA EtherChannel Bandwidth" section in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*).

Note After the port becomes a member of the PISA EtherChannel, only the **no channel-group 256 mode on** command has any effect on the port until the port is no longer a member of the PISA EtherChannel. While the port is a member of the PISA EtherChannel, all port configuration commands except the **no channel-group 256 mode on** command are ignored.

On a WS-S32-GE-PISA, you can allocate both ports 8 and 9 to the PISA EtherChannel.

You cannot enter any configuration under port channel interface 256.

The PISA EtherChannel MTU size is 4,096 bytes.

Examples

This example shows how to allocate the port ASIC capacity of port 3 to the PISA EtherChannel on a WS-S32-10GE-PISA that is installed in slot 5:

```
Router(config)# interface gigabitethernet 5/3
Router(config-if)# channel-group 256 mode on
Router(config-if)#
```

This example shows how to allocate the port ASIC capacity of port 9 to the PISA EtherChannel on a WS-S32-GE-PISA that is installed in slot 5:

```
Router(config)# interface gigabitethernet 5/9
Router(config-if)# channel-group 256 mode on
Router(config-if)#
```

This example shows how to revert to the default port ASIC capacity allocation.

```
Router(config)# interface gigabitethernet 5/9
Router(config-if)# no channel-group 256 mode on
Router(config-if)#
```

Related Commands

Command	Description
show interfaces	Displays the traffic that is seen by a specific interface.

interface port-channel

To create a port-channel virtual interface and enter interface configuration mode, use the **interface port-channel** command. To remove a virtual interface or subinterface, use the **no** form of this command.

interface port-channel *channel-number*[*.subinterface*]

no interface port-channel *channel-number*[*.subinterface*]

Syntax Description

channel-number	Channel number assigned to this port-channel interface; valid values are from 1 to 256.
.subinterface	(Optional) Subinterface number to be configured; valid values are from 0 to 4294967295.

Command Default

This command has no default settings.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is not supported on the IDSM and NAM.

This command is supported on EtherChannel, Fast EtherChannel, Gigabit EtherChannel, and 10-Gigabit EtherChannel interfaces.

The *channel-number* argument can be from 1 to 256, with a maximum of 128 port-channel interfaces.

You can create Layer 2 port channels dynamically or by entering the **interface port-channel** command; you can create Layer 3 port channels by entering the **interface port-channel** command only. You cannot create Layer 3 port channels dynamically.

Only one port channel in a channel group is allowed.

Ports can be bundled across any module.

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

When you use the **interface port-channel** command, follow these guidelines:

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

- If you do not assign a static MAC address on the port-channel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.

Examples

This example shows how to create a port-channel interface with a channel-group number of 256:

```
Router(config)# interface port-channel 256
Creating a switch port Po256. channel-group 256 is L2
Router(config-if)#
```

Note The port-channel interface counters that are shown by the **show counters interface port-channel** and **show interface port-channel counters** commands are not supported for channel groups that are using GE-WAN interfaces for QinQ link bundling. The **show interface port-channel** {*number* | *number.subif*} command (without the **counters** keyword) is supported, however.

Related Commands

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

interface range

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

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

Syntax Description

port-range	Port range; for a list of valid values for *port-range*, see the "Usage Guidelines" section for additional information.
macro *name*	Specifies the macro name.

Command Default

This command has no default settings.

Command Modes

Global or interface configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The values that you entered with the **interface range vlan** command are applied to all 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 port ranges that are created with the **interface range** command are not 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 slots.

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

You can enter the range with or without white spaces. For example, you can enter the range as **gigabitethernet 7/1 -7** or **gigabitethernet 7/1-7.**

When you enter a range of VLANs, any SVIs that do not exist within that range are created.

When entering the *port-range*, use this format: *card-type* {*slot*}/{*first-port*} - {*last-port*}.

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

- **ethernet**
- **fastethernet**
- **gigabitethernet**
- **loopback**

- **tengigabitethernet**
- **tunnel**
- **ge-wan**
- **pos**
- **atm**
- **vlan** *vlan-id* (valid values are from 1 to 4094)
- **port-channel** *interface-number* (valid values are from 1 to 256)

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

In addition, you can specify a single interface in *port-range*.

Examples

This example shows how to execute a command on two port ranges:

```
Router(config)# interface range fastethernet 5/18 -20, ethernet 3/1 -24
Router(config-if-range)#
```

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

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

Related Commands

Command	Description
define interface-range	Creates an interface-range macro.
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

interface vlan

To create or access a dynamic 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.

Command Default

Fast EtherChannel is not specified.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

If you delete an SVI by entering the **no interface vlan** *vlan-id* command, the associated IDB pair is forced into an administrative down state and is marked as deleted. The deleted interface will not be visible in the **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 is gone.

VLANs 1006 to 1014 are internal VLANs on the Catalyst 6500 series switch and cannot be used for creating new VLANs.

Examples

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

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

inter-packet gap 6502-mode

To set the IPG value, use the **inter-packet gap 6502-mode** command. To return to the default settings, use the **no** form of this command.

inter-packet gap 6502-mode

no inter-packet gap 6502-mode

Syntax Description

This command has no keywords or arguments.

Command Default

All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on situations where a WS-X6704-10GE is connected to a WS-X6502-10GE only. You enter this command to change the IPG value of the WS-X6704-10GE to match the WS-X6502-10GE.

The default 6704 mode sets the IPG value to average 12. Based on packet size, the IPG between successive packets range from 9 to 15.

The 6502 mode sets the IPG value to average 16. Based on packet size, the IPG between successive packets range from 13 to 19.

Examples

This example shows how to set the IPG to 6502 mode:

```
Router(config-if)# inter-packet gap 6502-mode
Router(config-if)#
```

This example shows how to set the IPG to the default mode:

```
Router(config-if)# no inter-packet gap 6502-mode
Router(config-if)#
```

ip access-list hardware permit fragments

To permit all noninitial fragments in the hardware, use the **ip access-list hardware permit fragments** command. To return to the default settings, use the **no** form of this command.

ip access-list hardware permit fragments

no ip access-list hardware permit fragments

Syntax Description

This command has no keywords or arguments.

Command Default

All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Flow fragments that match ACEs with Layer 4 ports and permit results are permitted in the hardware, and all other fragments are dropped. An entry is added in the TCAM for each ACE with Layer 4 ports and permit action. This action could cause large ACLs to not fit in the TCAM. If this situation occurs, use the **ip access-list hardware permit fragments** command to permit all noninitial fragments in the hardware.

This command affects all ACLs that are currently applied to interfaces and not only newly-applied ACLs.

The initial flow fragments that match the ACEs with Layer 4 ports and permit results are permitted in the hardware. All other initial fragments are dropped in the hardware.

Examples

This example shows how to permit all noninitial fragments in the hardware:

```
Router(config)# ip access-list hardware permit fragments
Router(config)#
```

This example shows how to return to the default settings:

```
Router(config)# no ip access-list hardware permit fragments
Router(config)#
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces that are configured for IP.

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) Treats implicit denies in the ARP ACL as explicit denies and drops packets that do not match any previous clauses in the ACL.

Command Default

No defined ARP ACLs are applied to any VLAN.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

For *vlan-range*, you can specify the VLAN to which the switches and hosts belong. You can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

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.

If you do not specify the **static** keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.

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

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection limit

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 return to the default settings, use the **no** form of this command.

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

no ip arp inspection limit

Syntax Description

rate *pps*	Specifies the upper limit on the number of incoming packets processed per second; valid values are from 1 to 2048 pps.
burst interval *seconds*	(Optional) Specifies the consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets; valid values are from 1 to 15 seconds.
none	Specifies that there is no upper limit on the rate of the incoming ARP packets that can be processed.

Command Default

The default settings are as follows:

- The **rate** *pps* 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** *seconds* is set to **1** second.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You should configure the trunk ports 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. You can use the error-disable timeout feature 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 on the 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:

```
Router# config terminal
Router(config)# interface fa6/3
Router(config-if)# ip arp inspection limit rate 25
Router(config-if)#
```

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:

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

Related Commands

Command	Description
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection log-buffer

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

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

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

Syntax Description

entries *number*	Specifies the number of entries from the logging buffer; valid values are from 0 to 1024.
logs *number*	Specifies the number of entries to be logged in an interval; valid values are from 0 to 1024.
interval *seconds*	Specifies the logging rate; valid values are from 0 to 86400 (1 day).

Command Default

The default settings are as follows:

- When dynamic ARP inspection is enabled, denied, or dropped, the ARP packets are logged.
- The **entries** *number* is **32**.
- The **logs** *number is* **5** per second.
- The **interval** *seconds is* **1** second.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

A **0** value for the **logs** *number* indicates that the entries should not be logged out of this buffer.

A **0** value for the **interval** *seconds* keyword and argument indicates an immediate log.

You cannot enter a **0** for both the **logs** *number* and the **interval** *seconds* keywords and arguments.

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. Registration for these packets occurs 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:

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer entries 45
Router(config)#
```

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

```
Router(config)# ip arp inspection log-buffer logs 10 interval 3
Router(config)#
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection log	Shows the status of the log buffer.

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.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

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

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

Related Commands

Command	Description
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection validate

To perform specific checks for an ARP inspection, use the **ip arp inspection validate** command. To disable ARP inspection 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.
dst-mac	(Optional) Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body.
ip	(Optional) Checks the ARP body for invalid and unexpected IP addresses.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

The **src-mac** checks are issued against both ARP requests and responses. The **dst-mac** checks are issued for ARP responses.

Note When enabled, packets with different MAC addresses are classified as invalid and are dropped.

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 no check options are enabled, all the checks are disabled.

Examples

This example shows how to enable the source MAC validation:

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

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection vlan

To enable 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.

Command Default

ARP inspection is disabled on all VLANs.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

For *vlan-range*, you can specify a single VLAN identified by a VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if the VLAN has not been created or is a private VLAN.

Examples

This example shows how to enable DAI on VLAN 1:

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

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip arp inspection vlan logging

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

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

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

Syntax Description

vlan-range	Number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.
acl-match	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
matchlog	Specifies that logging of packets matched against ACLs is controlled by the **matchlog** keyword in the permit and deny access control entries of the ACL.
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.

Command Default

All denied or dropped packets are logged.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

By default, the **matchlog** keyword is not available on the ACEs. When you enter the **matchlog** keyword, denied packets are not logged. Packets are logged only when they match against an ACE that has the **matchlog** keyword.

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 are as follows:

- **acl-match**—Logging on ACL matches is reset to log on deny
- **dhcp-bindings**—Logging on DHCP bindings 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 that matches the ACLs:

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

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

ip auth-proxy max-login-attempts

To limit the number of login attempts at a firewall interface, use the **ip auth-proxy max-login-attempts** command. To return to the default settings, use the **no** form of this command.

ip auth-proxy max-login-attempts *1-maxint*

no ip auth-proxy max-login-attempts

Syntax Description

1-maxint	Maximum number of login attempts: valid values are from 1 to 2147483647 attempts.

Command Default

1-maxint is **5**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on the firewall interfaces only.

The maximum login attempt functionality is independent of the watch-list feature. If you do not configure a watch list (using the **ip access-list hardware permit fragments** command) and you configure a maximum login attempt, the existing authentication proxy behavior occurs but displays the new number for retries. If you configure a watch list, the IP address is put in the watch list, once the configured number of attempts has been reached.

Examples

This example shows how to set a limit to the number of login attempts at a firewall interface:

```
Router(config-if)# ip auth-proxy max-login-attempts 4
Router(config-if)#
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

ip auth-proxy watch-list

To enable and configure an authentication proxy watch list, use the **ip auth-proxy watch-list** command. See the "Usage Guidelines" section for the **no** form of this command usage.

ip auth-proxy watch-list {{**add-item** *ip-addr*} | **enable** | {**expiry-time** *minutes*}}

no ip auth-proxy watch-list [{**add-item** *ip-addr*} | **expiry-time**]

Syntax Description

add-item *ip-addr*	Adds an IP address to the watch list.
enable	Enables a watch list.
expiry-time *minutes*	Specifies the duration of time that an entry is in the watch list; see the "Usage Guidelines" section for valid values.

Command Default

The defaults are as follows:

- *minutes* is **30** minutes.
- The watch-list functionality is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The valid values for minutes are from 0 to the largest 32-bit positive number (0x7FFFFFFF or 2147483647 in decimal). Setting the *minutes* to 0 (zero) places the entries in the list permanently.

This command is supported on the firewall interfaces only.

Use the **no** form of this command to do the following:

- **no ip auth-proxy watch-list**—Disables the watch-list functionality.
- **no ip auth-proxy watch-list add-item** *ip-addr*—Removes the IP address from the watch list.
- **no ip auth-proxy watch-list expiry-time**—Returns to the default setting.

A watch list consists of IP addresses that have opened TCP connections to port 80 and have not sent any data. No new connections are accepted from this type of IP address (to port 80) and the packet is dropped.

An entry remains in the watch list for the time that is specified by **expiry-time** *minutes*.

When you disable a watch list, no new entries are put into the watch list, but the sessions are put in SERVICE_DENIED state. The timer deletes sessions after 2 minutes.

Examples

This example shows how to enable an authentication proxy watch list:

```
Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#
```

This example shows how to disable an authentication proxy watch list:

```
Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#
```

This example shows how to add an IP address to a watch list:

```
Router(config-if)# ip auth-proxy watch-list add-item 12.0.0.2
Router(config-if)#
```

This example shows how to set the duration of time that an entry is in a watch list:

```
Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy max-login-attempts	Limits the number of login attempts at a firewall interface.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

ip casa

To configure the router to function as a forwarding agent, use the **ip casa** command. To disable the forwarding agent, use the **no** form of this command.

ip casa [*control-address igmp-address* [*udp-limit*]]

no ip casa

Syntax Description

control-address	(Optional) IP address of the forwarding agent side of the services manager and forwarding agent tunnel used for sending signals.
igmp-address	IGMP address on which the forwarding agent will listen for wildcard and fixed affinities.
udp-limit	(Optional) Maximum UDP queue length; valid values are from 50 to 65535.

Command Default

The default *udp-limit* value is 256.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If more than the maximum *udp-limit* value arrives in a burst, the CASA wildcard updates from the service manager might get dropped.

The *control-address* value is unique for each forwarding agent.

Examples

This example shows how to specify the IP address (10.10.4.1) and IGMP address (224.0.1.2) for the forwarding agent and set the UDP queue length to 300:

```
Router(config)# ip-casa 10.10.4.1 224.0.1.2 300
Router(config)#
```

Related Commands

Command	Description
forwarding-agent	Specifies the port on which the forwarding agent listens for the wildcard and the fixed affinities.

ip cef load-sharing algorithm

To select a CEF load-balancing algorithm, use the **ip cef load-sharing algorithm** command. To return to the default universal load-balancing algorithm, use the **no** form of this command.

ip cef load-sharing algorithm {**original** | **tunnel** [*id*] | **universal** [*id*]}

no ip cef load-sharing algorithm {**original** | **tunnel** [*id*] | **universal** [*id*]}

Syntax Description

original	Sets the load-balancing algorithm to the original based on a source and destination hash.
tunnel	Sets the load-balancing algorithm for use in tunnel environments or in environments where there are only a few IP source and destination address pairs.
universal	Sets the load-balancing algorithm to the universal algorithm that uses a source, destination, and ID hash.
id	(Optional) Fixed identifier.

Command Default

The universal load-balancing is selected.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The original CEF load-sharing algorithm produced distortions in load-balancing across multiple routers due to the use of the same algorithm on every router. When the load-balancing algorithm is set to universal mode, each router on the network can make a different load-balancing decision for each source-destination address pair which resolves load-balancing distortions.

Use the tunnel algorithm to share the load more fairly when only a few source-destination pairs are involved.

Examples

This example shows how to enable the CEF load-balancing algorithm for universal environments:

```
Router(config)# ip cef load-sharing algorithm universal 1
Router(config)#
```

Related Commands

Command	Description
ip load-sharing	Enables load balancing.

ip cef table consistency-check

To enable the CEF-table consistency-checker types and parameters, use the **ip cef table consistency-check** command. To disable consistency checkers, use the **no** form of this command.

ip cef table consistency-check [**type** {**lc-detect** | **scan-lc** | **scan-rib** | **scan-rp**}] [**count** *count-number*] [**period** *seconds*]

ip cef table consistency-check [**settle-time** *seconds*]

no ip cef table consistency-check [**type** {**lc-detect** | **scan-lc** | **scan-rib** | **scan-rp**}] [**count** *count-number*] [**period** *seconds*]

no ip cef table consistency-check [**settle-time** *seconds*]

Syntax Description

type	(Optional) Specifies the type of consistency check to configure.
lc-detect	(Optional) Specifies that the module detects a missing prefix.
scan-lc	(Optional) Specifies a passive scan check of tables on the module.
scan-rib	(Optional) Specifies a passive scan check of tables on the rendezvous point against RIB.
scan-rp	(Optional) Specifies a passive scan check of tables on the rendezvous point.
count *count-number*	(Optional) Specifies the maximum number of prefixes to check per scan; valid values are from 1 to 225.
period *seconds*	(Optional) Specifies the period between scans; valid values are from 30 to 3600 seconds.
settle-time *seconds*	(Optional) Specifies the time that elapsed during which updates for a candidate prefix are ignored as inconsistencies; valid values are from 1 to 3600 seconds.

Command Default

Enabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command configures CEF-table consistency checkers and parameters for the detection mechanism types that are listed in Table 2-12.

Table 2-12 Detection Mechanism Types

Mechanism	Operates On	Description
Lc-detect	Module	Operates on the module by retrieving IP prefixes found missing from its FIB table. If IP prefixes are missing, the module cannot forward packets for these addresses. Lc-detect sends IP prefixes to the rendezvous point for confirmation. If the rendezvous point detects that it has the relevant entry, an inconsistency is detected and a system message is displayed. Also, the rendezvous point sends a signal back to the module confirming that the IP prefix is an inconsistency.
Scan-lc	Module	Operates on the module by looking through the FIB table for a configurable time period and sending the next n prefixes to the rendezvous point. The rendezvous point does an exact lookup. If it finds the prefix missing, the rendezvous point reports an inconsistency. Finally, the rendezvous point sends a signal back to the module for confirmation.
Scan-rp	Route Processor	Operates on the rendezvous point (opposite of the scan-lc) by looking through the FIB table for a configurable time period and sending the next n prefixes to the module. The module does an exact lookup. If it finds the prefix missing, the module reports an inconsistency and finally signals the rendezvous point for confirmation.
Scan-rib	Route Processor	Operates on all RPs (even nondistributed) and scans the RIB to ensure that prefix entries are present in the rendezvous point FIB table.

Examples

This example shows how to enable the CEF-table consistency checkers:

```
Router(config)# ip cef table consistency-check
Router(config)#
```

Related Commands

Command	Description
clear ip cef inconsistency	Clears the statistics and records for the CEF-consistency checker.
show ip cef inconsistency	Displays the IP CEF inconsistencies.

ip dhcp relay information option trust-all

To enable all the interfaces as trusted sources of the DHCP relay-agent information option, use the **ip dhcp relay information option trust-all** command. To return to the default settings, use the **no** form of this command.

ip dhcp relay information option trust-all

no ip dhcp relay information option trust-all

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP server does not insert relay information.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is used by cable access router termination systems. This functionality enables a DHCP server to identify the user (cable access router) sending the request and initiate appropriate action that is based on this information.

Examples

This example shows how to specify that all interfaces on the router are trusted:

```
Router(config)# ip dhcp relay information option trust-all
Router(config)#
```

Related Commands

Command	Description
show ip dhcp relay information trusted-sources	Lists all the configured trusted interfaces.

ip dhcp relay information trust

To enable an interface as a trusted source of the DHCP relay-agent information, use the **ip dhcp relay information trust** command. To return to the default settings, use the **no** form of this command.

ip dhcp relay information trust

no ip dhcp relay information trust

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces on the router are untrusted.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Configuring an interface as a trusted source of relay-agent information allows the interface to receive DHCP discover or request packets. DHCP discover or request packets contain the relay-agent information option.

Examples

This example shows how to specify that the interface is trusted:

```
Router(config)# ip dhcp relay information trust
Router(config)#
```

Related Commands

Command	Description
show ip dhcp relay information trusted-sources	Lists all the configured trusted interfaces.

ip dhcp route connected

To specify routes as connected routes, use the **ip dhcp route connected** command. To return to the default settings, use the **no** form of this command.

ip dhcp route connected

no ip dhcp route connected

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces on the router are untrusted.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you enable the **ip dhcp route connected** command, DHCP downloads the route database from a database agent and adds the routes as connected routes, even though they may have been added as static routes previously.

Examples

This example shows how to specify routes as connected routes:

```
Router(config)# ip dhcp route connected
Router(config)#
```

ip dhcp snooping

To globally enable DHCP snooping, 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.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Wireless clients, or mobile nodes, gain access to an untrusted wireless network only if there is a corresponding entry in the DHCP snooping database. Enable DHCP snooping globally by entering the **ip dhcp snooping** command, and enable DHCP snooping on the tunnel interface by entering the **ip dhcp snooping packets** command. After you enable DHCP snooping, the process snoops DHCP packets to and from the mobile nodes and populates the DHCP snooping database.

Examples

This example shows how to enable DHCP snooping:

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

This example shows how to disable DHCP snooping:

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

Related Commands

Command	Description
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

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 interface-number*} {**expiry** *seconds*}

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

Syntax Description

mac-address	MAC address.
vlan *vlan*	Specifies a valid VLAN number; valid values are from 1 to 4094.
ip-address	IP address.
interface *interface*	Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**.
interface-number	Module and port number.
expiry *seconds*	Specifies the interval after which binding is no longer valid; valid values are from 1 to 4294967295 seconds.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When you add or remove a binding using this command, the binding database is marked as changed and a write is initiated.

A maximum of 512 bindings are allowed in the DHCP snooping database.

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:

```
Router# ip dhcp snooping binding 0000.0c00.40af vlan 1 10.42.0.6 interface gi1/1 expiry 1000
Router#
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping database

To configure the DHCP-snooping database, use the **ip dhcp snooping database** command.

ip dhcp snooping database {**bootflash:***url* | **ftp:***url* | **rcp**:*url* | **scp:***url* | **sup-bootflash:** | **tftp:***url*}

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

Syntax Description

bootflash:*url*	Specifies the database URL for storing entries using the bootflash.
ftp:*url*	Specifies the database URL for storing entries using FTP.
rcp:*url*	Specifies the database URL for storing entries using RCP.
scp:*url*	Specifies the database URL for storing entries using SCP.
sup-bootflash:	Specifies the database URL for storing entries using the supervisor engine bootflash.
tftp:*url*	Specifies the database URL for storing entries using TFTP.
timeout *timeout*	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
write-delay *time*	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default

This command has no default settings.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

Examples

This example shows how to specify the database URL using TFTP:

```
Router(config)# ip dhcp snooping database tftp://90.90.90.90/snooping-rp2
Router(config)#
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Router(config)# ip dhcp snooping database write-delay 15
Router(config)#
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

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 [**allow-untrusted**]

no ip dhcp snooping information option

Syntax Description

allow-untrusted	(Optional) Enables the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch.

Command Default

The defaults are as follows:

- **ip dhcp snooping information option**—Enabled
- **ip dhcp snooping information option allow-untrusted**—Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

DHCP option 82 is part of RFC 3046. DHCP is an application-layer protocol that is used for the dynamic configuration of TCP/IP networks. The protocol allows for a relay agent to pass DHCP messages between the DHCP clients and DHCP servers. By using a relay agent, servers do not have to be on the same network as the clients. Option 82 (82 is the option's code) addresses the security and scalability issues. Option 82 resides in the relay agent when DHCP packets that originate from the forwarding client are sent to the server. Servers that recognize option 82 may use the information to implement the IP address or other parameter assignment policies. The DHCP server echoes the option back to the relay agent in its replies. The relay agent strips out the option from the relay agent before forwarding the reply to the client.

When you enter the **ip dhcp snooping information option allow-untrusted** on an aggregation switch that is connected to an edge switch through an untrusted interface, the aggregation switch accepts packets with option 82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. You can enable the DHCP security features, such as dynamic ARP inspection or IP source guard, on the aggregation switch while the switch receives packets with option 82 information on untrusted input interfaces to which hosts are connected. You must configure the port on the edge switch that connects to the aggregation switch as a trusted interface.

⚠ **Caution** Do not enter the **ip dhcp snooping information option allow-untrusted** command on an aggregation switch that is connected to an untrusted device. If you enter this command, an untrusted device might spoof the option 82 information.

Examples

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

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

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

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

This example shows how to enable the switch to accept incoming DHCP snooping packets with option 82 information from the edge switch:

```
Router(config)# ip dhcp snooping information option allow-trusted
Router(config)#
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

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 message 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 that a switch can receive per second; valid values are from 1 to 4294967294 seconds.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on Layer 2 switch-port and port-channel interfaces only.

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 specify the number of DHCP messages that a switch can receive per second:

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

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

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

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping packets

To enable DHCP snooping on the tunnel interface, use the **ip dhcp snooping packets** command. To disable DHCP snooping, use the **no** form of this command.

ip dhcp snooping packets

no ip dhcp snooping packets

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on Layer 2 switch-port and port-channel interfaces only.

This command is supported on Catalyst 6500 series switches that are configured with a WLSM only.

Wireless clients, or mobile nodes, gain access to an untrusted wireless network only if there is a corresponding entry in the DHCP snooping database. Enable DHCP snooping globally by entering the **ip dhcp snooping** command, and enable DHCP snooping on the tunnel interface by entering the **ip dhcp snooping packets** command. After you enable DHCP snooping, the process snoops DHCP packets to and from the mobile nodes and populates the DHCP snooping database.

Examples

This example shows how to enable DHCP snooping:

```
Router(config)# ip dhcp snooping packets
Router(config)#
```

This example shows how to disable DHCP snooping:

```
Router(config)# no ip dhcp snooping packets
Router(config)#
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping verify mac-address

To verify that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify mac-address** command. To disable verification, use the **no** form of this command.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

For untrusted DHCP snooping ports, DHCP snooping verifies the MAC address on the client hardware address field to ensure that a client is requesting multiple addresses from a single MAC address. You can use the **ip dhcp snooping verify mac-address** command to trust the ports or you can use the **no ip dhcp snooping verify mac-address** command to leave the ports untrusted by disabling the MAC address verification on the client hardware address field.

Examples

This example shows how to verify that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port:

```
Router(config)# ip dhcp snooping verify mac-address
Router(config)#
```

This example shows how to turn off the verification of the MAC address on the client hardware address field:

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

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip dhcp snooping vlan

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

ip dhcp snooping vlan {*number* | *vlanlist*}

no ip dhcp snooping vlan {*number* | *vlanlist*}

Syntax Description

number | *vlanlist*	VLAN number or a group of VLANs; valid values are from 1 to 4094. See the "Usage Guidelines" section for additional information.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

Enter the range of VLANs using this format: 1,3-5,7,9-11.

Examples

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

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

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

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

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

```
Router(config)# ip dhcp snooping vlan 10,4-8,55
Router(config)#
```

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

```
Router(config)# no ip dhcp snooping vlan 10,4-8,55
Router(config)#
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

ip flow-aggregation cache

To create a flow-aggregation cache and enter the aggregation cache configuration mode, use the **ip flow-aggregation cache** command. To negate a command or return to its default settings, use the **no** form of this command.

ip flow-aggregation cache {**as** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix**}

no ip flow-aggregation cache {**as** | **destination-prefix** | **prefix** | **protocol-port** | **source-prefix**}

Syntax Description

as	Configures the autonomous-system aggregation-cache scheme.
destination-prefix	Configures the destination-prefix aggregation-cache scheme.
prefix	Configures the prefix aggregation-cache scheme.
protocol-port	Configures the protocol-port aggregation-cache scheme.
source-prefix	Configures the source-prefix aggregation-cache scheme.

Command Default

The defaults are as follows:

- **entries** *num* is 4096 entries.
- **active** *time* is 30 minutes.
- **inactive** *time* is 15 seconds.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

In source-prefix aggregation mode, only the source mask is configurable. In destination-prefix aggregation mode, only the destination mask is configurable.

Once you enter the flow aggregation cache configuration mode, these commands are available:

- **cache** {**entries** *num*} | {**timeout** {**active** *time*} | {**inactive** *time*}}
- **default** {**cache** {**entries** | **timeout**}} | **enabled** | {**export destination**}
- **enabled**
- **export destination** *ip-addr udp-port-num*

The syntax descriptions are as follows:

cache	Configures the NetFlow cache parameters.
entries *num*	Specifies the number of entries in the flow cache; valid values are from 1024 to 524288 flow entries.
timeout	Specifies the timeout parameters for the flow cache.
active *time*	Specifies the active flow timeout; valid values are from 1 to 60 minutes.
inactive *time*	Specifies the inactive flow timeout; valid values are from 10 to 600 seconds.
default	Sets a command to its default.
enabled	Enables the aggregation cache.
export destination	Specifies the host or port to send flow statistics.
ip-addr	Destination IP address or hostname.
udp-port-num	UDP port number; valid values are from 1 to 65535.

Examples

This example shows how to enable an autonomous-system aggregation-cache scheme:

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# enable
Router(config-flow-cache)#
```

Related Commands

Command	Description
show ip cache flow	Displays a summary of the NetFlow cache-flow entries.

ip flow-cache entries

To change the number of entries that are maintained in the NetFlow cache, use the **ip flow-cache entries** command. To return to the default number of entries, use the **no** form of this command.

ip flow-cache entries *number*

no ip flow-cache entries

Syntax Description

number	Number of entries to maintain in the NetFlow cache; valid values are from 1024 to 524288 entries.

Command Default

65536 entries

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Typically, the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries that are maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an Internet core router), we recommend that you maintain a larger value such as 131072. To obtain information on your flow traffic, use the **show ip cache flow** command.

Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time that a new flow is taken from the free-flow queue, the number of free flows is checked. If there are only a few free flows remaining, NetFlow attempts to age 30 flows using an accelerated timeout. If there is only one free flow remaining, NetFlow automatically ages 30 flows regardless of their age. This action ensures that free flow entries are always available.

Caution We recommend that you do not change the number of entries in the NetFlow cache. Improper use of this feature could cause network problems. To return to the default number of entries in the NetFlow cache, use the **no ip flow-cache entries** command.

Examples

This example shows how to increase the number of entries in the NetFlow cache to 131072:

```
Router(config)# ip flow-cache entries 131072
Router(config)# exit
```

Related Commands

Command	Description
show ip cache flow	Displays a summary of the NetFlow cache-flow entries.

ip flow-export

To globally enable NDE for the hardware-switched flows, use the **ip flow-export** command. To disable NDE for the hardware-switched flows, use the **no** form of this command.

ip flow-export

no ip flow-export

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are as follows:

- Disabled
- Version 7

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

To change the default NDE version, use the **ip flow-export hardware version** command.

Examples

This example shows how to enable NDE for the hardware-switched flows:

```
Router(config)# ip flow-export
Router(config)#
```

This example shows how to disable NDE for the hardware-switched flows:

```
Router(config)# no ip flow-export
Router(config)#
```

Related Commands

Command	Description
ip flow-export hardware version	Specifies the NDE version for hardware-switched flows.
show mls nde	Displays information about the NDE hardware-switched flow.

ip flow-export destination

To export the NetFlow cache entries to a specific destination, use the **ip flow-export destination** command. To disable information exporting, use the **no** form of this command.

ip flow-export destination {*hostname* | *ip-address*} *udp-port*

no ip flow-export destination

Syntax Description

hostname	IP hostname of the workstation to which you want to export the NetFlow information.
ip-address	IP address of the workstation to which you want to export the NetFlow information.
udp-port	UDP protocol-specific port number.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can enter two destination IP addresses to improve the probability of receiving complete NetFlow data by providing redundant data streams.

To configure multiple NetFlow export destinations to a router, enter the **ip flow-export destination** command twice, once for each destination. Do not enter the same IP address twice. However, entering two different IP addresses with the same UDP port number is configurable.

A NetFlow cache entry contains a lot of information. When flow switching is enabled with the **ip route-cache flow** command, you can use the **ip flow-export destination** command to configure the router to export the flow cache entry to a workstation when a flow expires. This feature can be useful for statistics, billing, and security, for example.

When entering the *ip-address* value, follow these guidelines:

- You cannot enter the IP address of the interface that you are currently on; you must use an address from the subnet of any interface that is not being used.
- You cannot use an address from a loopback interface; loopback interfaces do not have internal VLAN IDs or MAC addresses.

To specify the source IP address of the data, use the **ip flow-export source** command. To specify the version that is used on the workstation that receives the NetFlow data, use the **ip flow-export version** command.

For more information on NDE, refer to the “Configuring NDE” chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Examples

This example shows how to export a NetFlow cache entry to UDP port 125 using the version 1 format on the workstation that has an IP address of 10.42.42.1 99917:

```
Router# configure terminal
Router(config)# ip flow-export destination 10.42.42.1 9991 125
Router(config)# exit
```

Related Commands

Command	Description
ip flow-export source	Specifies the source interface IP address that is used in the NDE datagram.
ip flow-export version	Specifies the version for the export of information in NetFlow cache entries.
ip route-cache flow	Enables NetFlow switching for IP routing.

ip flow-export hardware version

To specify the NDE version for hardware-switched flows, use the **ip flow-export hardware version** command. To return to the default settings, use the **no** form of this command.

ip flow-export hardware version [**5** | **7**]

no ip flow-export hardware version

Syntax Description

5	Specifies that the export packet uses the version 5 format; see the "Usage Guidelines" section for additional information.
7	Specifies that the export packet uses the version 7 format; see the "Usage Guidelines" section for additional information.

Command Default

Version **7**

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to specify the NDE version for hardware-switched flows:

```
Router(config)# ip flow-export hardware version 5
Router(config)#
```

Related Commands

Command	Description
ip flow-export interface	Enables the interface-based ingress NDE for hardware-switched flows.
show mls nde	Displays information about the NDE hardware-switched flow.

ip flow-export interface

To enable the interface-based ingress NDE for hardware-switched flows, use the **ip flow-export interface** command. To disable interface-based NDE for hardware-switched flows, use the **no** form of this command.

ip flow-export interface

no ip flow-export interface

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use the **ip flow-export interface** command with the **ip flow ingress** command to enable or disable NDE on a specific interface.

Examples

This example shows how to enable interface-based NDE for hardware-switched flows:

```
Router(config)# ip flow-export interface
Router(config)#
```

This example shows how to disable interface-based NDE for hardware-switched flows:

```
Router(config)# no ip flow-export interface
Router(config)#
```

Related Commands

Command	Description
ip flow-export hardware version	Specifies the NDE version for hardware-switched flows.
show ip flow-export	Displays the information about the hardware-switched and software-switched flows for the data export, including the main cache and all other enabled caches.
show mls nde	Displays information about the NDE hardware-switched flow.

ip flow-export source

To specify the source interface IP address that is used in the NDE datagram, use the **ip flow-export source** command. To remove the source address, use the **no** form of this command.

ip flow-export source [{*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*}]

no ip flow-export source [{*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*}]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **ge-wan**, and **atm**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
port-channel *number*	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
vlan *vlan-id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.

Command Default

No source interface is specified.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

After you configure NDE, you can specify the source interface that is used in the UDP datagram containing the export data. The NetFlow Collector on the workstation uses the IP address of the source interface to determine which router sent the information. The NetFlow Collector performs SNMP queries to the router using the IP address of the source interface. Because the IP address of the source interface can change (for example, the interface might flap so a different interface is used to send the data), we recommend that you configure a loopback source interface. A loopback interface is always up and can respond to SNMP queries from the NetFlow Collector on the workstation.

For more information on NDE, refer to the "Configuring NDE" chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Examples

This example shows the configuration for a loopback source interface. The loopback interface has the IP address as 4.0.0.1 and is used by the serial interface in slot 5, port 0:

```
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ip address 4.0.0.1 255.0.0.0
Router(config-if)# exit
Router(config)# interface serial 5/0:0
Router(config-if)# ip unnumbered loopback0
Router(config-if)# no ip mroute-cache
Router(config-if)# encapsulation ppp
Router(config-if)# ip route-cache flow
Router(config-if)# exit
Router(config)# ip flow-export source loopback0
Router(config)# exit
```

Related Commands

Command	Description
ip flow-export destination	Exports the NetFlow cache entries to a specific destination.
ip flow-export version	Specifies the version for the export of information in NetFlow cache entries.
ip route-cache flow	Enables NetFlow switching for IP routing.

ip flow-export version

To specify the version for the export of information in NetFlow cache entries, use the **ip flow-export version** command. To return to the default settings, use the **no** form of this command.

ip flow-export version {**1** | {**5** [**origin-as** | **peer-as**]} | {**9** [**bgp-nexthop** | **origin-as** | **peer-as**]}}

no ip flow-export version

Syntax Description

1	Specifies that the export packet use the version 1 format; see the "Usage Guidelines" section for additional information.
5	Specifies that the export packet use the version 5 format; see the "Usage Guidelines" section for additional information.
origin-as	(Optional) Specifies that export statistics include the origin autonomous system for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer autonomous system for the source and destination.
9	Specifies that the export packet uses the version 9 format; see the "Usage Guidelines" section for additional information.
bgp-nexthop	(Optional) Specifies that export statistics include the BGP next hop for the source and destination.

Command Default

Export of information in NetFlow cache entries is disabled.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Version 5 and version 9 formats include the source and destination autonomous-system addresses and source and destination prefix masks. Also, version 9 includes BGP next-hop information.

The number of records stored in the datagram is a variable from 1 to 24 for version 1. The number of records stored in the datagram is a variable between 1 and 30 for version 5.

For more information on NDE, refer to the "Configuring NDE" chapter in the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Examples

This example shows how to export the data using the version 5 format:

```
Router(config)# ip flow-export version 5
Router(config)#
```

Related Commands

Command	Description
show mls nde	Displays information about the NDE hardware-switched flow.

ip flow ingress

To enable the software-switched flow creation in Layer 3, use the **ip flow ingress** command. To return to the default settings, use the **no** form of this command.

ip flow ingress

no ip flow ingress

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

To create a NetFlow entry, you need to enter the **ip flow ingress** command.

Follow these guidelines to display multicast entries:

- Enter the **show mls netflow ip** command.
- Enter the **ip flow ingress** command on an interface.
- Make sure that you have not entered the **no ip multicast netflow ingress** command.

Examples

This example shows how to enable inbound NDE for IPv4-bridged flows and NetFlow entry creation:

```
Router(config-if)# ip flow ingress
Router(config-if)#
```

This example shows how to disable inbound NDE for IPv4-bridged flows:

```
Router(config-if)# no ip flow ingress
Router(config-if)#
```

ip flow layer2-switched

To enable the creation of switched, bridged, and Layer 2 IP flows for a specific VLAN, use the **ip flow layer2-switched** command. To return to the default settings, use the **no** form of this command.

ip flow {**ingress** | **export**} **layer2-switched** {**vlan** {*num* | *vlanlist*}}

no ip flow {**ingress** | **export**} **layer2-switched** {**vlan** {*num* | *vlanlist*}}

Syntax Description

ingress	Enables the collection of switched, bridged, and IP flows in Layer 2.
export	Enables the export of switched, bridged, and IP flows in Layer 2.
vlan *num* | *vlanlist*	Specifies the VLAN or range of VLANs; valid values are from 1 to 4094. See the “Usage Guidelines” section for additional information.

Command Default

The defaults are as follows:

- **ip flow ingress layer2switch** is disabled.
- **ip flow export layer2switched** is enabled.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Before using this command, you must ensure that a corresponding VLAN interface is available and has a valid IP address.

You can enter one or multiple VLANs. The following examples are samples of valid VLAN lists: 1; 1,2,3; 1-3,7.

Examples

This example shows how to enable the collection of Layer 2-switched flows on a specific VLAN:

```
Router(config)# ip flow ingress layer2-switched vlan 2
Router(config)#
```

This example shows how to enable export of Layer 2-switched flows on a range of VLANs:

```
Router(config)# ip flow export layer2-switched vlan 1-3,7
Router(config)#
```

This example shows how to disable the collection of Layer 2-switched flows on a specific VLAN:

```
Router(config)# no ip flow ingress layer2-switched vlan 2
Router(config#
```

ip forward-protocol turbo-flood

To speed up the flooding of UDP packets using the spanning-tree algorithm, use the **ip forward-protocol turbo-flood** command. To return to the default settings, use the **no** form of this command.

ip forward-protocol turbo-flood [**udp-checksum**]

no ip forward-protocol turbo-flood [**udp-checksum**]

Syntax Description

udp-checksum	(Optional) Specifies the UDP checksum.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When you enter the **ip forward-protocol turbo-flood** command, the outgoing UDP packets have a NULL checksum. If you want to have UDP checksums on all outgoing packets, you must enter the **ip forward-protocol turbo-flood udp-checksum** command.

Examples

This example shows how to speed up the flooding of UDP packets using the spanning-tree algorithm:

```
Router(config)# ip forward-protocol turbo-flood
Router(config)#
```

This example shows how to speed up the flooding of UDP packets using the spanning-tree algorithm and have the UDP checksums on all outgoing packets:

```
Router(config)# ip forward-protocol turbo-flood udp-checksum
Router(config)#
```

This example shows how to turn off the **udp-checksum** keyword and the **ip forward-protocol turbo-flood** command:

```
Router(config)# no ip forward-protocol turbo-flood udp-checksum
Router(config)#
```

This example shows how to reinstate the **ip forward-protocol turbo-flood** command without the **udp-checksum** keyword:

```
Router(config)# ip forward-protocol turbo-flood
Router(config)#
```

Related Commands

Command	Description
ip forward-protocol	Specifies that protocols and ports that the router forwards when forwarding broadcast packets.

ip igmp immediate-leave group-list

To enable the immediate processing of the IGMP leave-group messages, use the **ip igmp immediate-leave group-list** command. To return to the default settings, use the **no** form of this command.

ip igmp immediate-leave group-list *acl*

no ip igmp immediate-leave group-list *acl*

Syntax Description

acl	Group ACL number; see the "Usage Guidelines" section for valid values.

Command Default

Disabled

Command Modes

Global or interface configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you enter the **ip igmp immediate-leave group-list** command, you must enter this command in VLAN interface configuration mode only.

Valid values for the *acl* argument are as follows:

- Access-list number—1 to 99
- Expanded range access-list number—1300 to 1999
- Name of the standard IP access list

You can configure one or the other but not both configuration modes at the same time.

You can enter the *acl* value to restrict the immediate-leave behavior to a simple access list for multicast groups. The IGMP leave-group messages for multicast groups that are not permitted by the *acl* value has the standard inquiry mechanism/leave latency.

Examples

This example shows how to enable the immediate processing of the IGMP leave-group messages:

```
Router(config)# ip igmp immediate-leave group-list 3
Router(config)#
```

ip igmp last-member-query-interval

To configure the last-member query interval for the IGMP, use the **ip igmp last-member-query-interval** command. To return to the default settings, use the **no** form of this command.

ip igmp last-member-query-interval *interval*

no ip igmp last-member-query-interval

Syntax Description

interval	Interval for the last-member query; valid values are from 100 to 65535 milliseconds in multiples of 100 milliseconds.

Command Default

1000 milliseconds (1 second); see the “Usage Guidelines” section for additional information.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Catalyst 6500 series switch waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If IGMP fast-leave processing is enabled and you enter the **no igmp last-member-query-interval** command, the interval is set to 0 seconds; immediate leave always assumes higher priority.

Examples

This example shows how to configure the last-member query interval to 200 milliseconds:

```
Router(config-if)# ip igmp last-member-query-interval 200
Router(config-if)#
```

Related Commands

Command	Description
ip igmp immediate-leave group-list	Enables the immediate processing of the IGMP leave-group messages.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

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

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are as follows:

- IGMP snooping is enabled on the Catalyst 6500 series switch.
- IGMP snooping is not configured on multicast routers.

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Before you can enable IGMP snooping on the Catalyst 6500 series switches, you must configure the VLAN interface for multicast routing.

Enter this command in VLAN interface configuration mode only.

Examples

This example shows how to enable IGMP snooping:

```
Router(config-if)# ip igmp snooping
Router(config-if)#
```

This example shows how to disable IGMP snooping:

```
Router(config-if)# no ip igmp snooping
Router(config-if)#
```

Related Commands

Command	Description
ip igmp snooping fast-leave	Enables the IGMPv3-snooping fast-leave processing.
ip igmp snooping mrouter	Configures a Layer 2 port as a multicast router port.
show ip igmp snooping explicit-tracking	Displays the information about the explicit host-tracking status for IGMPv3 hosts.

ip igmp snooping explicit-tracking

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

ip igmp snooping explicit-tracking

no ip igmp snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Modes

Enabled

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Explicit host tracking is supported only with IGMPv3 hosts.

When you enable explicit host tracking and the Catalyst 6500 series switch is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Catalyst 6500 series switch forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With IGMPv3 proxy reporting, the Catalyst 6500 series switch does proxy reporting for unsolicited reports and reports that are received in the general query interval.

Proxy reporting is turned on by default. When you disable proxy reporting, the Catalyst 6500 series switch works in transparent mode and updates the IGMP snooping database as it receives reports and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

IGMPv3 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN, the IGMP snooping software processes the IGMPv3 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that is reported by the host.
- The list of sources for each group that is reported by the hosts.
- The router filter mode of each group.
- For each group, the list of hosts that request the source.

Examples

This example shows how to enable IGMPv3-explicit host tracking:

```
Router(config-if)# ip igmp snooping explicit-tracking
Router(config-if)#
```

This example shows how to disable IGMPv3-explicit host tracking:

```
Router(config-if)# no ip igmp snooping explicit-tracking
Router(config-if)#
```

Related Commands

Command	Description
ip igmp snooping limit track	Limits the size of the explicit-tracking database.
show ip igmp snooping explicit-tracking	Displays the information about the explicit host-tracking status for IGMPv3 hosts.

ip igmp snooping fast-leave

To enable the IGMPv3-snooping fast-leave processing, use the **ip igmp snooping fast-leave** command. To disable fast-leave processing, use the **no** form of this command.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Syntax Description

This command has no arguments or keywords.

Command Modes

The defaults are as follows:

- IGMP version 2—Disabled
- IGMP version 3—Enabled

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Enter this command in VLAN interface configuration mode only.

Note Fast-leave processing is enabled by default. To disable fast-leave processing, you must enter the **no ip igmp snooping fast-leave** command to disable fast-leave processing.

You should use the IGMPv3-snooping fast-leave processing when there is a single receiver for the MAC group for a specific VLAN.

Examples

This example shows how to enable IGMPv3-snooping fast-leave processing:

```
Router(config-if)# ip igmp snooping fast-leave
Router(config-if)#
```

This example shows how to disable IGMPv3-snooping fast-leave processing:

```
Router(config-if)# no ip igmp snooping fast-leave
Router(config-if)#
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping explicit-tracking	Enables explicit host tracking.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.
show mac-address-table	Displays the information about the MAC-address table.

ip igmp snooping flooding

To configure periodic flooding of multicast packets, use the **ip igmp snooping flooding** command. To disable periodic flooding, use the **no** form of this command.

ip igmp snooping flooding [**timer** *seconds*]

no ip igmp snooping flooding

Syntax Description

timer *seconds*	(Optional) Specifies the interval between flooding in a 24-hour period for source-only entries; valid values are from 0 to 86400 seconds.

Command Modes

The defaults are as follows:

- Disabled.
- If enabled, *seconds* is **600** seconds (10 minutes).

Command Default

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on source-only VLANs.

You can enter **0** seconds to disable flooding. If you enter a maximum of 86400 seconds, flooding would occur once every 24 hours.

Examples

This example shows how to specify the interval between flooding in a 24-hour period:

```
Router(config-if)# ip igmp snooping flooding timer 300
Router(config-if)#
```

ip igmp snooping l2-entry-limit

To configure the maximum number of Layer 2 entries that can be created by the Catalyst 6500 series switch, use the **ip igmp snooping l2-entry-limit** command.

ip igmp snooping l2-entry-limit *max-entries*

Syntax Description

max-entries	Maximum number of Layer 2 entries that can be created by the Catalyst 6500 series switch; valid values are from 1 to 100000.

Command Default

15488 Layer 2 entries

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When entering *max-entries*, do not enter a comma (,).

Enter this command in VLAN interface configuration mode only.

Examples

This example shows how to configure the maximum number of Layer 2 entries that can be created by the Catalyst 6500 series switch:

```
Router(config-if)# ip igmp snooping l2-entry-limit 25000
Router(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

ip igmp snooping last-member-query-interval

To configure the last member query interval for IGMP snooping, use the **ip igmp snooping last-member-query-interval** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping last-member-query-interval *interval*

no ip igmp snooping last-member-query-interval

Syntax Description

interval	Interval for the last member query; valid values are from 100 to 900 milliseconds in multiples of 100 milliseconds.

Command Default

1000 milliseconds (1 second); see the "Usage Guidelines" section for additional information.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Catalyst 6500 series switch waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable IGMP fast-leave processing and you enter the **no igmp snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of **1000**. If you want this value, you must enter the **no ip igmp snooping last-member-query-interval** command and return to the default value (1000 milliseconds).

Examples

This example shows how to configure the last-member-query-interval to 200 milliseconds:

```
Router(config-if)# ip igmp snooping last-member-query-interval 200
Router(config-if)#
```

Related Commands

Command	Description
ip igmp snooping fast-leave	Enables the IGMP v3-snooping fast-leave processing.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

ip igmp snooping limit track

To limit the size of the explicit-tracking database, use the **ip igmp snooping limit track** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping limit track *max-entries*

no ip igmp snooping limit track

Syntax Description

max-entries	Maximum number of entries in the explicit-tracking database; valid values are from 0 to 128000 entries.

Command Default

max-entries is **32000**.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.

When you set the *max-entries* to **0**, explicit tracking is disabled.

When the explicit-tracking database exceeds the configured *max-entries*, a syslog message is generated.

When you reduce the *max-entries*, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

Examples

This example shows how to configure the maximum number of entries in the explicit-tracking database:

```
Router(config)# ip igmp snooping limit track 20000
Router(config)#
```

Related Commands

Command	Description
ip igmp snooping explicit-tracking	Enables explicit host tracking.
show ip igmp snooping explicit-tracking vlan	Displays information about the explicit host tracking for IGMPv3 hosts.

ip igmp snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ip igmp snooping mrouter** command. To remove the configuration., use the **no** form of this command

ip igmp snooping mrouter {**interface** {*interface interface-number*} |
{**port-channel** *number*}} | {**learn** {**cgmp** | **pim-dvmrp**}}

no ip igmp snooping mrouter {**interface** {*interface interface-number*} |
{**port-channel** *number*}} | {**learn** {**cgmp** | **pim-dvmrp**}}

Syntax Description

interface	Specifies the next-hop interface to the multicast router.
interface	Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values.
interface-number	Module and port number; see the "Usage Guidelines" section for valid values.
port-channel *number*	Specifies the port-channel number; valid values are a maximum of 64 values ranging from 1 to 256.
learn	Specifies the learning method for the multicast router.
cgmp	Specifies the snooping CGMP packets for the multicast router.
pim-dvmrp	Specifies the snooping PIM-DVMRP packets for the multicast router.

Command Default

pim-dvmrp

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Enter this command in VLAN interface configuration mode only.

The interface to the router must be in the VLAN where you are entering the command, the interface must be administratively up, and the line protocol must be up.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The CGMP learning method can decrease control traffic.

The learning method that you configure is saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

Examples

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

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

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

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

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping fast-leave	Enables the IGMPv3-snooping fast-leave processing.
show ip igmp snooping mrouter	Displays the information about the dynamically learned and manually configured multicast router interfaces.

ip igmp snooping querier

To enable multicast support within a subnet when no multicast routing protocol is configured in the VLAN or subnet, use the **ip igmp snooping querier** command. To disable multicast support within a subnet when no multicast routing protocol is configured, use the **no** form of this command.

ip igmp snooping querier

no ip igmp snooping querier

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Enter this command in VLAN interface configuration mode only.

You enable IGMP snooping on the Catalyst 6500 series switch, and disable PIM on the VLAN.

Configure the VLAN in global configuration mode.

Configure an IP address on the VLAN interface. When enabled, the IGMP-snooping querier uses the IP address as the query source address. If no IP address is configured on the VLAN interface, the IGMP-snooping querier does not start. The IGMP-snooping querier disables itself if you clear the IP address. When enabled, the IGMP-snooping querier restarts if you configure an IP address.

The IGMP-snooping querier supports IGMPv2.

When enabled, the IGMP-snooping querier does the following:

- Does not start if it detects IGMP traffic from a multicast router.
- Starts after 60 seconds when no IGMP traffic is detected from a multicast router.
- Disables itself if it detects IGMP traffic from a multicast router.

QoS does not support IGMP packets when IGMP snooping is enabled.

You can enable the IGMP-snooping querier on all the Catalyst 6500 series switches in the VLAN. One Catalyst 6500 series switch is elected as the querier.

If multicast routers are not present on the VLAN or subnet, the Catalyst 6500 series switch becomes the IGMP querier for the VLAN when you enable the IGMP-snooping querier.

If you disable the IGMP-snooping querier, IGMP snooping functions only when you configure PIM in the subnet.

You can enter the **ip igmp snooping querier** command at any time, but the IGMP-snooping querier starts only when no other multicast routers are present in the VLAN or subnet.

You can use this command as an alternative to configuring PIM in a subnet; use this command when the multicast traffic does not need to be routed but you would like support for IGMP snooping on Layer 2 interfaces in your network.

Examples

This example shows how to enable the IGMP-snooping querier on the VLAN:

```
Router(config-if)# ip igmp snooping querier
Router(config-if)#
```

Related Commands

Command	Description
show ip igmp snooping mrouter	Displays the information about the dynamically learned and manually configured multicast router interfaces.

ip igmp snooping rate

To set the rate limit for IGMP-snooping packets, use the **ip igmp snooping rate** command. To disable the software rate limiting, use the **no** form of this command.

ip igmp snooping rate *pps*

no ip igmp snooping rate

Syntax Description

pps	Rate limit of incoming IGMP messages; valid values are from 100 to 6000 packets per second.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to enable software rate limiting:

```
Router(config)# ip igmp snooping rate
Router(config)#
```

This example shows how to disable software rate limiting:

```
Router(config)# no ip igmp snooping rate
Router(config)#
```

Related Commands

Command	Description
show ip igmp snooping rate-limit	Displays the information about the IGMP snooping rate limit.

ip igmp snooping report-suppression

To turn on IP IGMP snooping report suppression, use the **ip igmp snooping report-suppression** command. To turn off report suppression, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When you enable report suppression for all host reports responding to a general query, IP IGMP snooping forwards the first report only and suppresses the remaining reports to constrain IGMP traffic to the multicast router.

ip igmp snooping source-only-learning age-timer

To flood multicast packets periodically to a Layer 2 segment that has only multicast sources and no receivers connected to it, use the **ip igmp snooping source-only-learning age-timer** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping source-only-learning age-timer *seconds*

no ip igmp snooping source-only-learning age-timer

Syntax Description

seconds	Source-only entries age timer value in seconds; valid values are from 0 to 86400 seconds.

Command Default

seconds is **600** seconds (10 minutes).

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

There are two source-only timers that run in an alternating fashion; the source_only_age_timer and the source_only_delete_timer. The value that you configure by entering the **ip igmp snooping source-only-learning age-timer** command sets the source_only_age_timer. The source_only_delete_timer has a fixed, nonconfigurable value of 5 minutes (300 seconds).

The expiration of one timer starts the other timer. At any time, only one timer is running.

Setting the age timer to **0** stops the flooding in the source-only VLAN.

Note Setting the age timer to a nonzero value causes flooding to occur every x (configured value) + 5 minutes (source_only_delete_timer) interval.

Examples

This example shows how to flood multicast packets periodically:

```
Router(config)# ip igmp snooping source-only-learning age-timer 300
Router(config)#
```

This example shows how to return to the default settings:

```
Router(config)# no ip igmp snooping source-only-learning age-timer
Router(config)#
```

ip igmp ssm-map

To enable and configure SSM mapping, use the **ip igmp ssm-map** command. To disable SSM mapping, use the **no** form of this command.

ip igmp ssm-map {**enable** | {**query dns**} | {**static** {*group-access-list* | *group-access-list-name*} *source-address*}}

no ip igmp ssm-map {**enable** | {**query dns**}

Syntax Description

enable	Enables SSM group to the source mapping.
query dns	Enables the DNS lookup.
static	Specifies an SSM static group to the source mapping.
group-access-list	Group access list to map to the source address.
group-access-list-name	Name of the group access list to map to the source address.
source-address	Source address.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

By default, the locally configured static SSM mappings and the DNS server are queried. Local configured mappings have priority over dynamic mappings. If a DNS server is not available, you may want to disable DNS server lookups. To disable DNS lookups, use the **no ip igmp ssm-map query dns** command.

If a DNS server is not available, a locally configured static SSM mapping database is used to query. A database query uses the group address and receives the source list in return. As soon as the static SSM mappings are configured, the maps are used for the lookups. To build a static SSM mappings database, use the following commands:

ip igmp ssm-map static *acl-1 source-1-ip-address*

ip igmp ssm-map static *acl-2 source-2-ip-address*

The ACL specifies the group or groups that have to be mapped to the listed source. Because the content servers may send out more then one stream with the same source address, the access list is used to group the multicast destination addresses together. You can use wildcards if the addresses are contiguous.

If multiple sources have to be joined for a multicast group address, you must place the group in all ACLs that are associated with the source address. In the example above, if group G must join sources 1 and 2, the group address must be placed in both acl-1 and acl-2.

When you enable SSM mapping using the **ip igmp ssm-map enable** command, but the source mapping list is empty for the group, enter the **no ip igmp ssm-map query dns** command. The **ip igmp ssm-map enable** command is supported on statically configured SSM-mapped source entries only.

Examples

This example shows how to enable an SSM group to the source mapping:

```
Router(config)# ip igmp ssm-map enable
Router(config)#
```

This example shows how to enable DNS lookups:

```
Router(config)# ip igmp ssm-map query dns
Router(config)#
```

This example shows how to build a static SSM mapping database:

```
Router(config)# ip igmp ssm-map static acl1 255.255.255.0
Router(config)# ip igmp ssm-map static acl2 255.255.255.0
Router(config)#
```

This example shows how to disable an SSM group to the source mapping:

```
Router(config)# no ip igmp ssm-map enable
Router(config)#
```

This example shows how to disable DNS lookups:

```
Router(config)# no ip igmp ssm-map query dns
Router(config)#
```

ip igmp tcn query

To configure the number of IGMP topology change queries to be executed during a set interval time, use the **ip igmp tcn query** command. To disable IGMP topology change queries, use the **no** form of this command.

ip igmp tcn query {**count** *count* | **interval** *interval*}

no ip igmp tcn query {**count** | **interval**}

Syntax Description

count *count*	Specifies the number of queries needed to stop flooding multicast traffic after a TCN event; valid values are from 1 to 10.
interval *interval*	Specifies the time until the IGMP TCN querier expires; valid values are from 1 to 255 seconds.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

Use **ip igmp tcn query count** command to control the time that multicast traffic is flooded after a TCN event. If you set the TCN flood query count to 1 by using the **ip igmp tcn query count** command, the flooding stops after receiving 1 general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Examples

This example shows how to set the number of queries to be executed:

```
Router(config)# ip igmp tcn query count 5
Router(config)#
```

This example shows how to set the time until the query expires to 120 seconds:

```
Router(config)# ip igmp tcn query interval 120
Router(config)#
```

ip local-proxy-arp

To enable local-proxy ARP, use the **ip local-proxy-arp** command. To disable local-proxy ARP, 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.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use local-proxy ARP on subnets where the hosts are intentionally prevented from communicating directly with each other; for example, you can use local-proxy ARP in private VLAN environments. Local-proxy ARP allows the PISA to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local-proxy ARP, the PISA can respond to ARP requests for IP addresses within a common subnet where traffic is not normally routed. This situation happens only when two hosts on the same subnet cannot directly ARP for each other.

ICMP redirects are disabled on interfaces where local-proxy ARP is enabled.

Examples

This example shows how to enable local-proxy ARP:

```
Router(config-if)# ip local-proxy-arp
Router(config-if)#s
```

ip mroute

To configure a multicast static route (mroute), use the **ip mroute** command. To remove the route, use the **no** form of this command.

ip mroute [**vrf** *vrf-name*] *source-address mask* [*protocol as-number*] {*rpf-address* | *interface-type interface-number*} [*distance*]

no ip mroute [**vrf** *vrf-name*] *source-address mask* [*protocol as-number*] {*rpf-address* | *interface-type interface-number*} [*distance*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
source-address	IP address of the multicast source.
mask	Mask on the IP address of the multicast source.
protocol	(Optional) Unicast routing protocol that you are using.
as-number	(Optional) Autonomous system number of the routing protocol that you are using, if applicable.
rpf-address	Incoming interface for the mroute.
interface-type interface-number	Interface type and number for the mroute.
distance	(Optional) Administrative distance; valid values are from 0 to 255.

Command Default

distance is **0**.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command allows you to statically configure where multicast sources are located (even though the unicast routing table shows something different).

When a source range is specified, the *rpf-address* argument applies only to those sources.

If the *rpf-address* is a PIM neighbor, PIM join, graft, and prune messages are sent to it. The *rpf-address* argument can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system. If the *rpf-address* argument is not specified, the interface *interface-type interface-number* value is used as the incoming interface.

The *distance* argument determines whether a unicast route, a DVMRP route, or a static mroute is used for the RPF lookup. The lower distances have a higher priority. If the static mroute has the same distance as the other two RPF sources, the static mroute will take precedence.

Examples

This example shows how to configure all sources from a single interface (in this case, a tunnel):

```
Router(config)# ip mroute 224.0.0.0 255.255.255.255 tunnel0
Router(config)#
```

This example shows how to configure all specific sources within a network number to be reachable through 172.30.10.13:

```
Router(config)# ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
Router(config)#
```

This example shows how to cause this multicast static route to take effect if the unicast routes for any given destination is deleted:

```
Router(config)# ip mroute 224.0.0.0 255.255.255.255 serial0 200
Router(config)#
```

ip msdp border

To configure a router that borders a PIM sparse-mode region and dense-mode region to use MSDP, use the **ip msdp border** command. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **border sa-address** *internet-type internet-number*

no ip msdp [**vrf** *vrf-name*] **border sa-address** *internet-type internet-number*

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
sa-address	Specifies an active source IP address.
internet-type internet-number	Interface type and number from which the IP address is derived and used as the rendezvous-point address in source-active messages.

Command Default

The active sources in the dense-mode region will not participate in MSDP.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command if you want the router to send source-active messages for sources active in the PIM dense-mode region to MSDP peers.

Specifying the *internet-type internet-number* allows the MSDP peers to forward source-active messages away from this border. The IP address of the interface is used as the originator ID, which is the rendezvous point field in the MSDP source-active message.

Note We recommend that you configure the border router in the sparse-mode domain to proxy-register sources in the dense-mode domain and configure the sparse-mode domain to use standard MSDP procedures to advertise these sources.

Note If you use this command, you must limit the sources advertised by using the **ip msdp redistribute** command. Configure the **ip msdp redistribute** command to apply to only local sources. Be aware that this configuration can result in an (S,G) state that remains long after a source in the dense-mode domain has stopped sending.

Note The **ip msdp originator-id** command identifies an interface type and number to be used as the rendezvous-point address. If both the **ip msdp border** and **ip msdp originator-id** commands are configured, the **ip msdp originator-id** command prevails. The address derived from the **ip msdp originator-id** command determines the address of the rendezvous point.

Examples

In this example, the local router is not a rendezvous point; it borders a PIM sparse-mode region with a dense-mode region and uses the IP address of Ethernet interface 0 as the rendezvous point address in source-active messages.

```
Router(config)# ip msdp border sa-address ethernet0
Router(config)#
```

Related Commands

Command	Description
ip msdp originator-id	Allows an MSDP speaker that originates a source-active message to use the IP address of the interface as the rendezvous-point address in the source-active message.
ip msdp redistribute	Configures which (S,G) entries from the multicast routing table are advertised in source-active messages originated to MSDP peers.

ip msdp cache-sa-state

To create a source-active state on the router, use the **ip msdp cache-sa-state** command.

ip msdp cache-sa-state [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.

Command Modes

The router creates the source-active state for all MSDP source-active messages that it receives.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is automatically configured if at least one MSDP peer is configured. It cannot be disabled.

Examples

This example shows how the **ip msdp cache-sa-state** command is enabled when an MSDP peer is configured. For more MSDP configuration examples, refer to the "Configuring Multicast Source Discovery Protocol" chapter in the Cisco IOS Release 12.2 *Cisco IOS IP Configuration Guide*.

```
.
.
.
Router(config)# ip classless
Router(config)# ip msdp peer 192.168.1.2 connect-source Loopback0
Router(config)# ip msdp peer 192.169.1.7
Router(config)# ip msdp mesh-group outside-test 192.168.1.2
Router(config)# ip msdp cache-sa-state
Router(config)# ip msdp originator-id Loopback0
.
.
.
```

Related Commands

Command	Description
clear ip msdp sa-cache	Configures an MSDP peer.
ip msdp filter-sa-request	Creates a source-active state on the router.
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

ip msdp default-peer

To define a default peer from which to accept all MSDP source-active messages, use the **ip msdp default-peer** command. To remove the default peer, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*]

no ipip msdp [**vrf** *vrf-name*] **default-peer**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-address | *peer-name*	IP address or DNS name of the MSDP default peer.
prefix-list *list*	(Optional) Specifies the BGP prefix list.

Command Modes

No default MSDP peer exists.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use the **ip msdp default-peer** command if you do not want to configure your MSDP peer to be a BGP peer also.

If only one MSDP peer is configured (with the **ip msdp peer** command), it will be used as a default peer. You do not need to configure a default peer with this command.

If you do not specify the **prefix-list** *list* keyword and argument, all source-active messages that are received from the configured default peer are accepted.

The **prefix-list** *list* keyword and argument specifies that the peer will be a default peer only for the prefixes listed in the list specified by the *list* argument. You must configure a BGP prefix list for this **prefix-list** *list* keyword and argument to have any effect.

You should configure a BGP prefix list if you intend to configure the **prefix-list** *list* keyword and argument with the **ip msdp default-peer** command.

If you specify the **prefix-list** *list* keyword and argument, the source-active messages that originated from the rendezvous points that are covered by the **prefix-list** *list* keyword and argument are accepted from the configured default peer. If you specify the **prefix-list** *list* keyword and argument but do not configure a prefix list, the default peer is used for all prefixes.

You can enter multiple **ip msdp default-peer** commands, with or without the **prefix-list** keyword. However, all commands must either have the keyword or all must not have the keyword.

- When you use multiple **ip msdp default-peer** commands with the **prefix-list** keyword, you use all the default peers at the same time for different rendezvous-point prefixes. This syntax is typically used in a service provider cloud that connects stub site clouds.
- When you use multiple **ip msdp default-peer** commands without the **prefix-list** keyword, you use a single active peer to accept all source-active messages. If that peer goes down, then you move to the next configured default peer to accept all source-active messages. This syntax is typically used at a stub site.

Examples

This example shows how to configure the router named router.cisco.com as the default peer to the local router:

```
Router(config)# ip msdp peer 192.168.1.2
Router(config)# ip msdp peer 192.168.1.3
Router(config)# ip msdp default-peer router.cisco.com    !At a stub site
```

This example shows how to configure the router at IP address 192.168.1.3 as the default peer to the local router:

```
Router(config)# ip msdp peer 192.168.1.3
Router(config)# ip msdp peer 192.168.3.5
Router(config)# ip msdp default-peer 192.168.1.3
```

This example shows how to configure two default peers:

```
Router(config)# ip msdp peer 172.18.2.3
Router(config)# ip msdp peer 172.19.3.5
Router(config)# ip msdp default-peer 172.18.2.3 prefix-list site-c
Router(config)# ip prefix-list site-a permit 172.18.0.0/16
Router(config)# ip msdp default-peer 172.19.3.5 prefix-list site-a
Router(config)# ip prefix-list site-c permit 172.19.0.0/16
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip prefix-list	Creates an entry in a prefix list.

ip msdp description

To add descriptive text to the configuration for an MSDP peer, use the **ip msdp description** command. To remove the description, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **description** {*peer-name* | *peer-address*} *text*

no ip msdp [**vrf** *vrf-name*] **description** {*peer-name* | *peer-address*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-name | *peer-address*	Peer name or address to which this description applies.
text	Description of the MSDP peer.

Command Modes

No description is associated with an MSDP peer.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Configure a description to make the MSDP peer easier to identify. This description is displayed in the output of the **show ip msdp peer** command.

Examples

This example shows how to configure the router at the IP address 224.107.5.4 with a description indicating it is a router at customer A:

```
Router(config)# ip msdp description 224.107.5.4 router at customer a
Router(config)#
```

Related Commands

Command	Description
show ip msdp peer	Displays detailed information about the MSDP peer.

ip msdp filter-sa-request

To configure the router to send source-active request messages to the MSDP peer when a new joiner from a group becomes active, use the **ip msdp filter-sa-request** command. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*]

no ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address* | *peer-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-address	IP address of the MSDP peer from which the local router requests source-active messages when a new joiner for the group becomes active.
peer-name	Name of the MSDP peer from which the local router requests source-active messages when a new joiner for the group becomes active.
list *access-list*	(Optional) Specifies the standard IP access-list number or name that describes a multicast group address.

Command Modes

If this command is not configured, all source-active request messages are recognized. If this command is configured but no access list is specified, all source-active request messages are ignored.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

By default, the router recognizes all source-active request messages from peers. Use this command if you want to control exactly which source-active request messages that the router will recognize.

If no access list is specified, all source-active request messages are ignored. If an access list is specified, only source-active request messages from those permitted groups will be recognized, and all others will be ignored.

Examples

This example shows how to configure the router to filter source-active request messages from the MSDP peer at 172.16.2.2. This example also shows that the source-active request messages from sources on the network 192.168.22.0 pass access list 1 and will be recognized; all others will be ignored.

```
Router(config)# ip msdp filter sa-request 224.69.2.2 list 1
access-list 1 permit 228.4.22.0 0.0.0.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp mesh-group

To configure an MSDP peer to be a member of a mesh group, use the **ip msdp mesh-group** command. To remove an MSDP peer from a mesh group, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address* | *peer-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
mesh-name	Name of the mesh group.
peer-address | *peer-name*	IP address or name of the MSDP peer to be a member of the mesh group.

Command Modes

The MSDP peers do not belong to a mesh group.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. The source-active messages received from a peer in a mesh group are not forwarded to the other peers in the same mesh group.

The mesh groups can be used to achieve two goals:

- Reduce source-active message flooding
- Simplify peer-RPF flooding (you do not need to run BGP or multiprotocol BGP among MSDP peers)

Examples

This example shows how to configure the MSDP peer at address 224.1.1.1 to be a member of the mesh group named internal:

```
Router(config)# ip msdp mesh-group internal 224.1.1.1
Router(config)#
```

ip msdp originator-id

To allow an MSDP speaker that originates a source-active message to use the IP address of the interface as the rendezvous-point address in the source-active message, use the **ip msdp originator-id** command. To prevent the rendezvous-point address from being derived in this way, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

no ip msdp [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
interface-type *interface-number*	Interface type and number on the local router whose IP address is used as the rendezvous-point address in source-active messages.

Command Modes

The rendezvous-point address is used as the originator ID.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **ip msdp originator-id** command identifies an interface type and number to be used as the rendezvous-point address in a source-active message.

Use this command if you want to configure a logical rendezvous point. Because only rendezvous points and MSDP border routers originate source-active messages, you might need to change the ID used for this purpose.

If both the **ip msdp border sa-address** and **ip msdp originator-id** commands are configured, the **ip msdp originator-id** command prevails. The address derived from the **ip msdp originator-id** command determines the address of the rendezvous point to be used in the source-active message.

Examples

This example shows how to configure the IP address of Ethernet interface 1 as the rendezvous-point address in source-active messages:

```
Router(config)# ip msdp originator-id ethernet1
Router(config)#
```

Related Commands

Command	Description
ip msdp border	Configures a router that borders a PIM sparse-mode region and dense-mode region to use MSDP.

ip msdp peer

To configure an MSDP peer, use the **ip msdp peer** command. To remove the peer relationship, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type interface-number*] [**remote-as** *as-number*]

no ip msdp [**vrf** *vrf-name*] **peer** {*peer-name* | *peer-address*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-name | *peer-address*	DNS name or IP address of the router that is to be the MSDP peer.
connect-source *interface-type interface-number*	(Optional) Specifies the interface type and number whose primary address becomes the source IP address for the TCP connection.
remote-as *as-number*	(Optional) Specifies the autonomous system number of the MSDP peer.

Command Modes

No MSDP peer is configured.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The router specified should also be configured as a BGP neighbor.

The *interface-type* is on the router being configured.

If you are also using BGP peering with this MSDP peer, you should use the same IP address for MSDP that you used for BGP. However, you are not required to run BGP or multiprotocol BGP with the MSDP peer if there is a BGP or MBGP path between the MSDP peers. If there is no path, you must configure the **ip msdp default-peer** command.

The **remote-as** *as-number* keyword and argument is used for display purposes only.

A peer might appear to be in another autonomous system (other than the one it really resides in) when you have an MSDP peering session but do not have a BGP peer session with that peer. In this case, if the prefix of the peer is injected by another autonomous system, it displays as the autonomous system number of the peer.

Examples

This example shows how to configure the router at the IP address 224.108.1.2 as an MSDP peer to the local router. The neighbor belongs to autonomous system 109.

```
Router(config)# ip msdp peer 224.108.1.2 connect-source ethernet 0
router bgp 110
 network 224.108.0.0
 neighbor 224.108.1.2 remote-as 109
 neighbor 224.108.1.2 update-source ethernet 0
```

This example shows how to configure the router named router.cisco.com as an MSDP peer to the local router:

```
Router(config)# ip msdp peer router.cisco.com
Router(config)#
```

This example shows how to configure the router named router.cisco.com to be an MSDP peer in autonomous system 109. The primary address of Ethernet interface 0 is used as the source address for the TCP connection.

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet0 remote-as 109
Router(config)#
```

Related Commands

Command	Description
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

ip msdp redistribute

To configure which (S,G) entries from the multicast routing table are advertised in source-active messages originated to MSDP peers, use the **ip msdp redistribute** command. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **redistribute** [**list** *access-list-name*] [**asn** *as-access-list-number*] [**route-map** *map-name*]

no ip msdp [**vrf** *vrf-name*] **redistribute**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
list *access-list-name*	(Optional) Specifies the standard or extended IP access-list number or name that controls which local sources are advertised and to which groups they send.
asn *as-access-list-number*	(Optional) Specifies the standard or extended IP access-list number; valid values are from 1 to 199.
route-map *map-name*	(Optional) Specifies the route-map name.

Command Modes

The default settings are as follows:

- If no portion of this command is configured, only local sources are advertised, provided that they send to groups for which the router is a rendezvous point.
- If no portion of this command is configured and if the **ip msdp border sa-address** command is configured, all local sources are advertised.
- If the **ip msdp redistribute** command is configured with no keywords, no multicast sources are advertised.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must configure the *as-access-list-number* argument in the **ip as-path** command.

This command affects source-active message origination, not source-active message forwarding. If you want to filter which source-active messages are forwarded to MSDP peers, use the **ip msdp sa-filter in** or **ip msdp sa-filter out** command.

The **ip msdp redistribute** command controls which (S,G) pairs the router advertises from the multicast routing table. By default, only sources within the local domain are advertised. Use the following guidelines for the **ip msdp redistribute** command:

- If you specify the **list** *access-list-name* keyword and argument only, you filter which local sources are advertised and to which groups are sent advertisements. The access list specifies a source address, source mask, group address, and group mask.
- If you specify the **asn** *as-access-list-number* keyword and argument only, you advertise all sources sending to any group that pass through the autonomous system path access list. The autonomous system path access-list number refers to the **ip as-path** command, which specifies an access list. If you specify the **asn 0** keywords, sources from all autonomous systems are advertised. The **asn 0** keywords are useful when connecting dense-mode domains to a sparse-mode domain running MSDP, or when using MSDP in a router that is not configured with BGP. In these cases, you do not know if a source is local.
- If you specify the **route-map** *map-name* keyword and argument only, you advertise all sources that satisfy the match criteria in the route map *map-name* argument.
- If you specify all three keywords (**list**, **asn**, and **route-map**), all conditions must be true before any multicast source is advertised in a source-active message.
- If you specify the **ip multicast redistribute** command with no other keywords or arguments, no multicast sources are advertised.

Examples

This example shows how to configure which (S,G) entries from the multicast routing table are advertised in source-active messages originated to MSDP peers:

```
Router(config)# ip msdp redistribute route-map customer-sources

route-map customer-sources permit
match as-path customer-as

Router(config)# ip as-path access-list ^109$
```

Related Commands

Command	Description
ip as-path	Defines a BGP autonomous system path access list.
ip msdp border	Configures a router that borders a PIM sparse-mode region and dense-mode region to use MSDP.

ip msdp sa-filter in

To configure an incoming filter list for source-active messages received from the specified MSDP peer, use the **ip msdp sa-filter in** command. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*]

no ip msdp [**vrf** *vrf-name*] **sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the source-active messages are filtered.
list *access-list-name*	(Optional) Specifies the IP access-list number or name.
route-map *map-name*	(Optional) Specifies the route-map name.

Command Modes

The default settings are as follows:

- If this command is not configured, no incoming messages are filtered; all source-active messages are accepted from the peer.
- If the command is configured, but no access list or route map is specified, all source/group pairs from the peer are filtered.
- If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S,G) pair in incoming source-active messages.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you do not specify an *access-list-name*, all source/group pairs from the peer are filtered.

The specified MSDP peer passes only those source-active messages that meet the match criteria in the route map *map-name* argument.

If all match criteria are true, a **permit** keyword from the route map passes the routes through the filter. Use the **deny** keyword to filter the routes.

Examples

This example shows how to configure the router to filter all source-active messages from the peer named router.cisco.com:

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet 0
Router(config)# ip msdp sa-filter in router.cisco.com
Router(config)#
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter out	Configures an outgoing filter list for source-active messages sent to the specified MSDP peer.

ip msdp sa-filter out

To configure an outgoing filter list for source-active messages sent to the specified MSDP peer, use the **ip msdp sa-filter out** command. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*]

no ip msdp [**vrf** *vrf-name*] **sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-address | *peer-name*	IP address or DNS name of the MSDP peer to which the source-active messages are filtered.
list *access-list*	(Optional) Specifies the extended IP access-list number or name.
route-map *map-name*	(Optional) Specifies the route map name.

Command Modes

The default settings are as follows:

- If this command is not configured, no outgoing messages are filtered; all source-active messages received are forwarded to the peer.
- If the command is configured, but no access list or route map is specified, all source/group pairs are filtered.
- If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S,G) pairs in outgoing source-active messages.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you do not specify an *access-list*, all source/group pairs are filtered. The specified MSDP peer passes only those source-active messages that pass the extended access list.

If both the **list** and **route-map** keywords are used, all conditions must be true to pass any (S,G) pairs in outgoing source-active messages.

To the specified MSDP peer, only those source-active messages that meet the match criteria in the route map *map-name* argument are passed.

If all match criteria are true, a **permit** keyword from the route map passes routes through the filter. Use the **deny** keyword to filter the routes.

Examples

This example shows how to allow only (S,G) pairs that pass access list 100 to be forwarded in a source-active message to the peer named router.cisco.com:

```
Router(config)# ip msdp peer router.cisco.com connect-source ethernet 0
Router(config)# ip msdp sa-filter out router.cisco.com list 100
access-list 100 permit ip 224.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter in	Configures an incoming filter list for source-active messages received from the specified MSDP peer.

ip msdp sa-request

To configure the router to send source active request messages to the MSDP peer when a new joiner from the group becomes active, use the **ip msdp sa-request** command. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address* | *peer-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests source-active messages when a new joiner for the group becomes active.

Command Modes

The router does not send source-active request messages to the MSDP peer.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

By default, the router does not send any source-active request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member waits to receive any source-active messages that eventually arrive.

Use this command if you want a new member of a group to learn the current, active multicast sources in a connected PIM-SM domain that are sending to a group. The router sends source-active request messages to the specified MSDP peer when a new member joins a group. The peer replies with the information in its source-active cache. If the peer does not have a cache configured, this command does not work.

You can also use the **ip msdp cache-sa-state** command to have the router cache messages.

Examples

This example shows how to configure the router to send source-active request messages to the MSDP peer at 224.69.1.1:

```
Router(config)# ip msdp sa-request 224.69.1.1
Router(config)#
```

Related Commands

Command	Description
ip msdp cache-sa-state	Creates a source-active state on the router.
ip msdp peer	Configures an MSDP peer.

ip msdp shutdown

To administratively shut down a configured MSDP peer, use the **ip msdp shutdown** command. To bring the peer back up, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address* | *peer-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-address | *peer-name*	IP address or name of the MSDP peer to shut down.

Command Modes

No action is taken to shut down an MSDP peer.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to shut down the MSDP peer at the IP address 224.5.7.20:

```
Router(config)# ip msdp shutdown 224.5.7.20
Router(config)#
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp ttl-threshold

To limit which multicast data packets are sent in source-active messages to an MSDP peer, use the **ip msdp ttl-threshold** command. To restore the default value, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **ttl-threshold** {*peer-address* | *peer-name*} *ttl-value*

no ip msdp [**vrf** *vrf-name*] **ttl-threshold** {*peer-address* | *peer-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
peer-address | *peer-name*	IP address or name of the MSDP peer to which the *ttl-value* argument applies.
ttl-value	Time-to-live (TTL) value; valid values are from 0 to 255.

Command Default

ttl-value is **0**.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command limits which multicast data packets are sent in data-encapsulated source-active messages. Only multicast packets with an IP header TTL greater than or equal to the *ttl-value* argument are sent to the MSDP peer that is specified by the IP address or name.

Use this command if you want to use TTL to limit your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, you need to send those packets with a TTL greater than 8.

The default value of the *ttl-value* argument is 0, which means that all multicast data packets are forwarded to the peer until the TTL is exhausted.

Examples

This example shows how to configure a TTL threshold of eight hops:

```
Router(config)# ip msdp ttl-threshold 224.5.7.20 8
Router(config)#
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip multicast boundary

To configure an administratively scoped boundary, use the **ip multicast boundary** command. To remove the boundary, use the **no** form of this command.

ip multicast boundary *access-list* [**filter-autorp**]

no ip multicast boundary *access-list* [**filter-autorp**]

Syntax Description

access-list	Number or name that identifies an access list that controls the range of group addresses affected by the boundary.
filter-autorp	(Optional) Filters auto RP messages denied by the boundary ACL.

Command Default

There is no boundary.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command to configure an administratively scoped boundary on an interface to filter the multicast group addresses in the range that is defined by the *access-list* argument. A standard access list defines the range of addresses affected. When you configure this command, multicast data packets are not allowed to flow across an interface from either direction. Restricting the multicast data packet flow enables reuse of the same multicast group address in different administrative domains.

Note Extended access lists are not allowed with the **filter-autorp** keyword or the use of **no** keywords.

If you configure the **filter-autorp** keyword, the administratively scoped boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Use the following guidelines when you enter the **ip multicast boundary** command:

- Only standard access lists are permitted with the use of the **filter-autorp** keyword or **no** keyword.
- All instances of the command apply to both control and data plane traffic.
- Protocol information on the extended access list is parsed to allow reuse and filtering for IOS consistency. An (S,G) operation will be filtered by an extended access list under all conditions stated above for keywords if the access list filters (S,G) traffic for all protocols.

Examples

This example shows how to set up a boundary for all administratively scoped addresses:

```
Router(config-if)# ip multicast boundary 1
Router(config-if)#
```

This example shows how to set up a boundary for an extended ACL:

```
Router(config-if)# ip multicast boundary 101
Router(config-if)#
```

This example shows how to filter auto RP messages denied by the boundary ACL.

```
Router(config-if)# ip multicast boundary acc_grp10 filter-autorp
Router(config-if)#
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.

ip multicast cache-headers

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** command. To remove the buffer, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **cache-headers** [**rtp**]

no ip multicast [**vrf** *vrf-name*] **cache-headers**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
rtp	(Optional) Caches RTP headers.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can store IP multicast packet headers in a cache and then display them to determine the following information:

- Who is sending IP multicast packets to which groups
- Interpacket delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Size of the group
- UDP port numbers
- Packet length

Note This command allocates a circular buffer of approximately 32 KB. Do not configure this command if you are low on memory.

Use the **show ip mpacket** command to display the buffer.

Examples

This example shows how to allocate a buffer to store IP multicast packet headers:

```
Router(config)# ip multicast cache-headers
Router(config)#
```

Related Commands

Command	Description
show ip mpacket	Displays the contents of the circular cache-header buffer.

ip multicast helper-map

To allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks, use the **ip multicast helper-map** command. To disable this function, use the **no** form of this command.

ip multicast helper-map broadcast *multicast-address access-list* [**ttl** *x*]

no ip multicast helper-map broadcast *multicast-address access-list*

Syntax Description

broadcast	Specifies that the traffic is being converted from broadcast to multicast. Use this keyword with the *multicast-address* argument.
multicast-address	IP multicast address to which the converted traffic is directed. Use this argument with the **broadcast** keyword.
access-list	IP-extended access-list number or name that controls which broadcast packets are translated, based on the UDP port number.
ttl *x*	(Optional) Translates packets with a TTL of 1 and resets the TTL; valid values are from 1 to 50.

Command Default

No conversion between broadcast and multicast occurs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When a multicast-capable internetwork is between two broadcast-only internetworks, you can convert the broadcast traffic to multicast at the first-hop router, and convert it back to broadcast at the last-hop router before delivering the packets to the broadcast clients. However, broadcast packets with the IP source address of 0.0.0.0 (such as a DHCP request) are not translated to any multicast group.

If you send a directed broadcast to the subnet, the outgoing interface of the last-hop router can be configured with an IP broadcast address of x.x.x.255, where x.x.x.0 is the subnet that you are trying to reach; otherwise, the packet is converted to 255.255.255.255.

Broadcast packets with a TTL of 1 are not translated by the **ip multicast helper-map** command unless you use the **ttl** keyword with the command.

Examples

This example shows how to allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks:

```
Router(config-if)# ip multicast helper-map broadcast 224.5.5.5 120 ttl 2
Router(config-if)#
```

Related Commands

Command	Description
ip directed-broadcast	Enables the translation of a directed broadcast to physical broadcasts.
ip forward-protocol turbo-flood	Speeds up the flooding of UDP packets using the spanning-tree algorithm.

ip multicast mrinfo-filter

To filter multicast router information (mrinfo) request packets, use the **ip multicast mrinfo-filter** command. To disable this configuration, use the **no** form of this command.

ip multicast mrinfo-filter *access-list*

no ip multicast mrinfo-filter *access-list*

Syntax Description

access-list	Access list of the source IP address to be filtered.

Command Modes

This command has no default settings.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **ip multicast mrinfo-filter** command filters the mrinfo request packets for all of the sources listed in the specified access list.

Examples

This example shows how to specify that mrinfo request packets are filtered for all sources that are listed in access-list number 4:

```
Router(config)# ip multicast mrinfo-filter 4
Router(config)#
```

ip multicast multipath

To split the load of IP multicast traffic across multiple equal-cost paths, use the **ip multicast multipath** command. To disable this configuration, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **multipath**

no ip multicast [**vrf** *vrf-name*] **multipath**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.

Command Default

If multiple equal-cost paths exist, multicast traffic will not be split across these paths.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you enter the **ip multicast multipath** command and multiple equal-cost paths exist in your network, load splitting will occur across the equal-cost paths for multicast traffic from different sources to the same multicast group, but not for traffic from the same source to different multicast groups. Because this command changes the way a RPF neighbor is selected, you must split the load of IP multicast traffic across equal-cost paths consistently on all routers in a redundant topology to avoid looping.

Examples

This example shows how to split the load of IP multicast traffic across multiple equal-cost paths:

```
Router(config)# ip multicast multipath
Router(config)#
```

Related Commands

Command	Description
show ip rpf	Displays the triggered RPF statistics.

ip multicast netflow

To enable multicast egress or ingress NetFlow accounting on an interface, use the **ip multicast netflow** command. To disable multicast NetFlow accounting, use the **no** form of this command.

ip multicast netflow {**egress** | **ingress**}

no ip multicast netflow {**egress** | **ingress**}

Syntax Description

egress	Specifies multicast egress NetFlow accounting.
ingress	Specifies multicast ingress NetFlow accounting.

Command Default

The defaults are as follows:

- Multicast egress NetFlow accounting is disabled.
- Multicast ingress NetFlow accounting is enabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The output of the **show running-config** command does not indicate when multicast ingress accounting is enabled (but it does indicate when multicast ingress NetFlow accounting is disabled).

You must enable multicast egress NetFlow accounting on all interfaces for which you want to count outgoing multicast stream.

To display the multicast entries, enter the **show mls netflow ip** command.

Examples

This example shows how to enable multicast ingress NetFlow accounting on the ingress Ethernet 1/0 interface:

```
Router# configure terminal
Router(config)# interface ethernet 1/0
Router(config-if)# ip multicast netflow ingress
Router(config-if)# end
```

Related Commands

Command	Description
ip multicast netflow rpf-failure	Enables NetFlow accounting for multicast data that fails the RPF check.
show ip flow interfaces	Displays NetFlow accounting configuration on interfaces.

ip multicast route-limit

To limit the number of multicast routes (mroutes) that can be added to a multicast routing table, use the **ip multicast route-limit** command. To disable this configuration, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

no ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
limit	Number of mroutes that can be added; valid values are from 1 to 2147483647.
threshold	(Optional) Number of mroutes that cause a warning message to occur; valid values are from 1 to 2147483647.

Command Modes

limit is 2147483647.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **ip multicast route-limit** command limits the number of multicast routes that can be added to a router and generates an error message when the limit is exceeded. If you set the *threshold* argument, a threshold error message is generated when the threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the *limit* argument.

The mroute warning *threshold* must not exceed the mroute *limit*.

Examples

This example shows how to set the mroute limit at 200,000 and the threshold at 20,000 for a VRF instance named cisco:

```
Router(config)# ip multicast vrf cisco route-limit 200000 20000
Router(config)#
```

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command. To disable IP multicast routing, use the **no** form of this command.

ip multicast-routing [**vrf** *vrf-name*] [**distributed**]

no ip multicast-routing [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
distributed	(Optional) Enables MDS.

Command Default

This command is disabled.

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When IP multicast routing is disabled, no multicast packets are forwarded.

Examples

This example shows how to enable IP multicast routing:

```
Router(config)# ip multicast-routing
Router(config)#
```

This example shows how to enable IP multicast routing on a specific VRF:

```
Router(config)# ip multicast-routing vrf vrf1
Router(config)#
```

This example shows how to disable IP multicast routing:

```
Router(config)# no ip multicast-routing
Router(config)#
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip multicast rpf backoff

To set the PIM-backoff interval, use the **ip multicast rpf backoff** command. To return to the default settings, use the **no** form of this command.

ip multicast rpf backoff {{*min max*} | **disable**}

no ip multicast rpf backoff

Syntax Description

min	Initial RPF-backoff delay in milliseconds; valid values are from 1 to 65535 milliseconds.
max	Maximum RPF-backoff delay in milliseconds; valid values are from 1 to 65535 milliseconds.
disable	Disables the triggered RPF check.

Command Modes

If you enable the triggered RPF check, the defaults are as follows:

- *min* is **500** milliseconds.
- *max* is **5000** milliseconds.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you do not enable the triggered RPF check, PIM periodically polls the routing tables for changes (set using the **ip multicast rpf interval** command). When you enable the triggered RPF check, PIM polls the routing tables when a change in the routing tables occurs. The *min* argument sets the initial backoff time. Once triggered, PIM waits for additional routing table changes. If the *min* period expires without further routing table changes, PIM scans for routing changes. If additional routing changes occur during the backoff period, PIM doubles the length of the backoff period. You can set the maximum interval for the doubled backoff period with the *max* argument.

Use this command in the following situation:

- You have frequent route changes in your device (for example, on a dial-in router).
- You want to either reduce the maximum RPF-check interval for faster availability of IP multicast on newly established routes, or you want to increase the RPF-check interval to reduce the CPU load that is introduced by the RPF check.

Examples

This example shows how to set the PIM-backoff interval in milliseconds:

```
Router(config)# ip multicast rpf backoff 100
Router(config)#
```

Related Commands

Command	Description
ip multicast rpf interval	Sets the RPF consistency-check interval.
show ip rpf events	Displays the triggered RPF statistics.

ip multicast rpf interval

To set the RPF consistency-check interval, use the **ip multicast rpf interval** command. To return to the default settings, use the **no** form of this command.

ip multicast rpf interval *interval*

no ip multicast rpf interval

Syntax Description

interval	Interval in seconds between RPF checks; valid values are from 1 to 10 seconds.

Command Default

10 seconds

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **ip multicast rfp interval** command sets the interval PIM and polls the routing tables for changes.

Examples

This example shows how to set the RPF consistency-check interval in seconds:

```
Router(config)# ip multicast rpf interval 5
Router(config)#
```

Related Commands

Command	Description
ip multicast rpf backoff	Sets the PIM-backoff interval.

ip pim accept-register

To configure a candidate rendezvous-point router to filter PIM register messages, use the **ip pim accept-register** command. To disable this function, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

no ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
list *access-list*	Specifies the extended access-list number or name.
route-map *map-name*	Specifies the route-map name.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command to prevent unauthorized sources from registering with the rendezvous point. If an unauthorized source sends a register message to the rendezvous point, the rendezvous point immediately sends a register-stop message.

Examples

This example shows how to restrict the rendezvous point from allowing sources in the SSM range of addresses to register with the rendezvous point. These statements need to be configured only on the rendezvous point.

```
Router(config)# ip pim accept-register list no-ssm-range
Router(config)# ip access-list extended no-ssm-range
 deny ip any 232.0.0.0 0.255.255.255
 permit ip any any
Router(config)#
```

ip pim accept-rp

To configure a router to accept join or prune messages that are destined for a specified rendezvous point and for a specific list of groups, use the **ip pim accept-rp** command. To remove the check, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-rp** {*rp-address* | **auto-rp**} [*access-list*]

no ip pim [**vrf** *vrf-name*] **accept-rp** {*rp-address* | **auto-rp**} [*access-list*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
rp-address	Address of the rendezvous point that is allowed to send join messages to groups in the range specified by the group access list.
auto-rp	Specifies that join and register messages are accepted only for rendezvous points that are in the Auto-RP cache.
access-list	(Optional) Access-list number or name that defines which groups are subject to the check.

Command Default

Disabled—All join messages and prune messages are processed.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command causes the router to accept only (*, G) join messages that are destined for the specified rendezvous-point address. Additionally, the group address must be in the range specified by the access list.

When the *rp-address* argument is one of the addresses of the system, the system is the rendezvous point only for the specified group range specified by the access list. When the group address is not in the group range, the rendezvous point does not accept join or register messages and responds immediately to register messages with register-stop messages.

Examples

This example shows how to configure the router to accept join or prune messages that are destined for the rendezvous point at address 172.17.1.1 for the multicast group 224.2.2.2:

```
Router(config)# ip pim accept-rp 172.17.1.1 3
access-list 3 permit 224.2.2.2
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.

ip pim bidir-enable

To enable bidir-PIM, use the **ip pim bidir-enable** command. To disable bidir-PIM, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bidir-enable**

no ip pim [**vrf** *vrf-name*] **bidir-enable**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When bidir-PIM is disabled, the switch operates similarly to a router without bidir-PIM support. The following conditions apply:

- PIM hello messages that are sent by the router do not contain the bidirectional mode option.
- The router does not send designated forwarder election messages and ignores designated forwarder election messages that are received.
- The **ip pim rp-address**, **ip pim send-rp-announce**, and **ip pim rp-candidate** commands are treated as follows:
  - If these commands are configured when bidir-PIM is disabled, bidirectional mode is not a configuration option.
  - If these commands are configured with the bidirectional mode option when bidir-PIM is enabled and then bidir-PIM is disabled, these commands are removed from the CLI. You must enter these commands again with the bidirectional-mode option when you reenable bidir-PIM.
- The **df** keyword for the **show ip pim interface** command is not supported.

Examples

This example shows how to enable bidir-PIM:

```
Router(config)# ip pim bidir-enable
Router(config)#
```

This example shows how to disable bidir-PIM:

```
Router(config)# no ip pim bidir-enable
Router(config)#
```

Related Commands

Command	Description
ip pim rp-address	Configures the address of a PIM rendezvous point for a particular group.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR.
ip pim send-rp-announce	Uses Auto-RP to configure groups for which the router acts as a rendezvous point.

ip pim bsr-candidate

To configure the router to announce its candidacy as a BSR, use the **ip pim bsr-candidate** command. To remove this router as a candidate bootstrap router, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority*]

no ip pim [**vrf** *vrf-name*] **bsr-candidate**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
interface-type interface-number	Interface type and number on this router from which the BSR address is derived to make it a candidate.
hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called.
priority	(Optional) BSR priority; valid values are from 0 to 255.

Command Default

The default settings are as follows:

- Disabled.
- If enabled, the *priority* is **0**.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command causes the router to send bootstrap messages to all its PIM neighbors with the address of the designated interface as the BSR address. Each neighbor compares the BSR address with the address it had from previous bootstrap messages (not necessarily received on the same interface). If the current address is the same or higher address, it caches the current address and forwards the bootstrap message. Otherwise, the router drops the bootstrap message.

This router continues to be the BSR until it receives a bootstrap message from another candidate BSR saying that it has a higher priority (or if the same priority, a higher IP address).

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. A stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good BSR candidate.

You must enable the *interface-type* with PIM.

When setting the *hash-mask-length* argument, all groups with the same seed hash correspond to the same rendezvous point. For example, if this value is 24, only the first 24 bits of the group addresses are applicable; using this setting allows you to get one rendezvous point for multiple groups.

When setting the *priority*, the BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR.

Examples

This example shows how to configure the IP address of the router on Ethernet interface 0 to be a candidate BSR with a priority of 10:

```
Router(config)# ip pim bsr-candidate ethernet 0 10
Router(config)#
```

Related Commands

Command	Description
ip pim bsr border	Prevents BSR messages from being sent or received through an interface.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR.
ip pim send-rp-discovery	Configures the router as a rendezvous-point mapping agent.
show ip pim bsr	Displays the BSR information.
show ip pim rp	Displays active rendezvous points that are cached with associated multicast routing entries.

ip pim register-rate-limit

To set a limit on the maximum number of PIM-SM register messages that are sent per second for each (S,G) routing entry, use the **ip pim register-rate-limit** command. To disable this limit, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **register-rate-limit** *rate*

no ip pim [**vrf** *vrf-name*] **register-rate-limit**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
rate	Maximum number of register messages that are sent per second by the router; valid values are from 1 to 65535 messages per second.

Command Default

No limit is defined.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command to limit the number of register messages that the designated router allows for each (S,G) entry. Enabling this command limits the load on the designated router and rendezvous point but drops those register messages that exceed the set limit. Receivers may experience data packet loss within the first second in which register messages are sent from bursty sources.

If you enter the **ip pim dense-mode proxy-register** command, then you must enter the **ip pim register-rate-limit** command because of the potentially large number of sources from the dense-mode area that may send data into the sparse-mode region (and need registering in the border router).

This command applies only to sparse mode (S,G) multicast routing entries.

Examples

This example shows how to set a limit on PIM-SM register messages with a maximum rate of two register messages per second:

```
Router(config)# ip pim register-rate-limit 2
Router(config)#
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim register-source

To configure the IP source address of a register message to an interface address other than the outgoing interface address of the designated router leading toward the rendezvous point, use the **ip pim register-source** command. To disable this configuration, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **register-source** *interface-type interface-number*

no ip pim [**vrf** *vrf-name*] **register-source**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
interface-type interface-number	Interface type and interface number that identify the IP source address of a register message.

Command Default

The IP address of the outgoing interface of the designated router leading toward the rendezvous point is used as the IP source address of a register message.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is required only when the IP source address of a register message is not a uniquely routed address to which the rendezvous point can send packets. This situation may occur if the source address is filtered so that packets sent to it are not forwarded or if the source address is not unique to the network. In these cases, the replies sent from the rendezvous point to the source address fail to reach the designated router and result in PIM-SM protocol failures.

If you do not configure an IP source address or if the configured source address is not in service, the IP address of the outgoing interface of the designated router leading to the rendezvous point is used as the IP source address of the register message. We recommend that you use a loopback interface with an IP address that is uniquely routed throughout the PIM-SM domain.

Examples

This example shows how to configure the IP source address of the register message to the loopback 3 interface of a designated router:

```
Router(config)# ip pim register-source loopback 3
Router(config)#
```

ip pim rp-announce-filter

To filter incoming Auto-RP announcement messages coming from the rendezvous point, use the **ip pim rp-announce-filter** command. To remove the filter, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-announce-filter rp-list** *access-list* **group-list** *access-list*

no ip pim [**vrf** *vrf-name*] **rp-announce-filter rp-list** *access-list* **group-list** *access-list*

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
rp-list *access-list*	Specifies the number or name of a standard access list of rendezvous-point addresses that are allowable for the group ranges supplied in the **group-list** *access-list* combination.
group-list *access-list*	Specifies the number or name of a standard access list that describes the multicast groups that the RPs serve.

Command Default

All rendezvous-point announcements are accepted.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Configure this command on the PIM rendezvous-point mapping agent. We recommend that if you use more than one rendezvous-point mapping agent, make the filters among them consistent so that there are no conflicts in the mapping state when the announcing agent is removed.

Examples

This example shows how to configure the router to accept rendezvous-point announcements from rendezvous points in access list 1 for group ranges that are described in access list 2:

```
Router(config)# ip pim rp-announce-filter rp-list 1 group-list 2
Router(config)#
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.

ip pim rp-candidate

To configure the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR, use the **ip pim rp-candidate** command. To remove this router as a rendezvous-point candidate, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-type interface-number* [**group-list** *access-list*] [**bidir**]

no ip pim [**vrf** *vrf-name*] **rp-candidate**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
interface-type interface-number	IP address associated with this interface type and number is advertised as a candidate rendezvous-point address.
group-list *access-list*	(Optional) Specifies the standard IP access-list number or name that defines the group prefixes that are advertised with the rendezvous-point address.
bidir	(Optional) Indicates that the multicast groups that are specified by the *access-list* argument operate in bidirectional mode.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command causes the router to send a PIM Version 2 message advertising itself as a rendezvous-point candidate to the BSR. The addresses allowed by the access list, together with the router identified by the type and number, constitute the rendezvous point and its range of addresses for which it is responsible.

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. A stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good rendezvous-point candidate.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using the PIM Version 2 BSR mechanism to distribute group-to-rendezvous point mappings. Other options are as follows:

- If you are using Auto-RP to distribute group-to-rendezvous point mappings, use the **bidir** keyword with the **ip pim send-rp-announce** command.
- If you are not distributing group-to-rendezvous point mappings using either Auto-RP or the PIM Version 2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

The *access-list* name cannot contain a space or quotation mark and must begin with an alphabetic character to avoid confusion with numbered access lists.

If you enter this command without the **bidir** keyword, the groups that are specified operate in PIM sparse mode.

Examples

This example shows how to configure the router to advertise itself as a rendezvous-point candidate to the BSR in its PIM domain. Standard access-list number 4 specifies the group prefix that is associated with the rendezvous point that has the address identified by Ethernet interface 2. That rendezvous point is responsible for the groups with the prefix 239.

```
Router(config)# ip pim rp-candidate 192.168.37.33 ethernet 2 group-list 4
access-list 4 permit 239.0.0.0 0.255.255.255
Router(config)#
```

Related Commands

Command	Description
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim rp-announce-filter	Filters incoming Auto-RP announcement messages coming from the rendezvous point.
ip pim send-rp-announce	Uses Auto-RP to configure groups for which the router acts as a rendezvous point.

ip pim send-rp-announce

To use Auto-RP to configure groups for which the router will act as a rendezvous point, use the **ip pim send-rp-announce** command. To deconfigure this router as a rendezvous point, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-type interface-number* **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]

no ip pim [**vrf** *vrf-name*] **send-rp-announce**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
interface-type interface-number	Interface type and number that is used to define the rendezvous-point address.
scope *ttl-value*	Time-to-live (TTL) value that limits the number of Auto-RP announcements; valid values are from 1 to 255.
group-list *access-list*	(Optional) Specifies the standard IP access-list number or name that defines the group prefixes that are advertised in association with the rendezvous-point address.
interval *seconds*	(Optional) Specifies the interval between rendezvous-point announcements in seconds; valid values are from 1 to 16383 seconds.
bidir	(Optional) Indicates that the multicast groups that are specified by the *access-list* argument operate in bidirectional mode.

Command Default

The default settings are as follows:

- Auto-RP is disabled.
- If enabled, the *seconds* is 60 seconds.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this command in the router that you want as a rendezvous point. When you are using Auto-RP to distribute group-to-rendezvous point mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a rendezvous-point candidate for the groups in the range that are described by the access list.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using Auto-RP to distribute group-to-rendezvous point mappings. Other options are as follows:

- If you are using the PIM Version 2 bootstrap router (PIMv2 BSR) mechanism to distribute group-to-rendezvous point mappings, use the **bidir** keyword with the **ip pim rp-candidate** command.
- If you are not distributing group-to-rendezvous point mappings using either Auto-RP or the PIMv2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

If you enter this command without the **bidir** keyword, the specified groups operate in PIM-SM.

The *access-list* name cannot contain a space or quotation mark and must begin with an alphabetic character to avoid confusion with numbered access lists.

The total holdtime of the rendezvous-point announcements is automatically set to three times the value of the interval.

Examples

This example shows how to send rendezvous-point announcements out all PIM-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as a rendezvous point is the IP address that is associated with Ethernet interface 0. Access list 5 describes the groups for which this router serves as a rendezvous point.

```
Router(config)# ip pim send-rp-announce ethernet0 scope 31 group-list 5
access-list 5 permit 224.0.0.0 15.255.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip pim rp-address	Configures the address of a PIM rendezvous point for a particular group.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 rendezvous-point candidate to the BSR.

ip pim send-rp-discovery

To configure the router as a rendezvous-point mapping agent, use the **ip pim send-rp-discovery** command. To restore the default value, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value*

no ip pim [**vrf** *vrf-name*] **send-rp-discovery**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
interface-type interface-number	(Optional) Interface type and number that is used to define the rendezvous-point mapping agent address.
scope *ttl-value*	Specifies the time-to-live (TTL) value in the IP header that keeps the discovery messages within this number of hops; valid values are from 1 to 255.

Command Default

The router is not a rendezvous-point mapping agent.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Configure this command on the router that is designated as a rendezvous-point mapping agent. Specify a TTL large enough to cover your PIM domain.

When Auto-RP is used, the following occurs:

1. The rendezvous-point mapping agent listens on well-known group address CISCO-RP-ANNOUNCE (224.0.1.39), to which rendezvous-point candidates send.
2. The rendezvous-point mapping agent sends rendezvous point-to-group mappings in an Auto-RP rendezvous point discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40). The TTL value limits how many hops that the message can take.
3. PIM-designated routers listen to this group and use the rendezvous points that they learn about from the discovery message.

Examples

This example shows how to limit Auto-RP rendezvous-point discovery messages to 20 hops:

```
Router(config)# ip pim send-rp-discovery scope 20
Router(config)#
```

ip pim snooping (global configuration mode)

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

ip pim snooping

no ip pim snooping

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

PIM snooping is not supported on groups that are connected to the reserved MAC address range (for example, 0100.5e00.00xx).

When you disable PIM snooping globally, PIM snooping is disabled on all VLANs.

Examples

This example shows how to enable PIM snooping globally:

```
Router(config)# ip pim snooping
Router(config)#
```

This example shows how to disable PIM snooping globally:

```
Router(config)# no ip pim snooping
Router(config)#
```

Related Commands

Command	Description
show ip pim snooping	Displays the information about IP PIM snooping.

ip pim snooping (interface configuration mode)

To enable PIM snooping on an interface, use the **ip pim snooping** command. To disable PIM snooping on an interface, use the **no** form of this command.

ip pim snooping

no ip pim snooping

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

PIM snooping is not supported on groups that are connected to the reserved MAC address range (for example, 0100.5e00.00xx).

You must enable PIM snooping globally before enabling PIM snooping on an interface. When you disable PIM snooping globally, PIM snooping is disabled on all VLANs.

You can enable PIM snooping on VLAN interfaces only.

Examples

This example shows how to enable PIM snooping on a VLAN interface:

```
Router(config)# interface vlan 101
Router(config-if)# ip pim snooping
Router(config-f)#
```

This example shows how to disable PIM snooping on a VLAN interface:

```
Router(config-if)# no ip pim snooping
Router(config-f)#
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping dr-flood

To enable flooding of the packets to the designated router, use the **ip pim snooping dr-flood** command. To disable the flooding of the packets to the designated router, use the **no** form of this command.

ip pim snooping dr-flood

no ip pim snooping dr-flood

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

PIM snooping is not supported on groups that are connected to the reserved MAC address range (for example, 0100.5e00.00xx).

Enter the **no ip pim snooping dr-flood** command only on switches that have no designated routers attached.

The designated router is programmed automatically in the (S,G) O-list.

Examples

This example shows how to enable flooding of the packets to the designated router:

```
Router(config)# ip pim snooping dr-flood
Router(config)#
```

This example shows how to disable flooding of the packets to the designated router:

```
Router(config)# no ip pim snooping dr-flood
Router(config)#
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping suppress sgr-prune

To enable suppression of SGR-prune packets to the designated router, use the **ip pim snooping suppress sgr-prune** command in global configuration mode. To disable the suppression of the packets to the designated router, use the **no** form of this command.

ip pim snooping suppress sgr-prune

no ip pim snooping suppress sgr-prune

Syntax Description

This command has no arguments or keywords.

Command Default

The suppression of packets to the designated router is disabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(18)ZY	This command was introduced.
12.2(18)SXF	This command was introduced.

Usage Guidelines

If a shared tree and SPT diverge in a VLAN on your switch router, and you have PIM snooping configured, then duplicate multicast packets may be delivered in your network. PIM snooping may stop the prune message sent by the receiver from reaching the upstream switch router in the shared tree, which causes more than one upstream switch router to forward the multicast traffic. This situation causes duplicate multicast packets to be delivered to the receivers. The sending of duplicate multicast packets only lasts a couple of seconds because the PIM-ASSERT mechanism is initiated and stops the extraneous flow. However, the cycle repeats itself when the next prune message is sent. To stop this situation from occurring, enter the **no ip pim snooping suppress sgr-prune** command.

Examples

The following example shows how to enable suppression of the SGR-prune packets to the designated router:

```
Router(config)# ip pim snooping suppress sgr-prune
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim spt-threshold

To configure when a PIM leaf router should join the shortest path source tree for the specified group, use the **ip pim spt-threshold** command. To restore the default value, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
kbps	Traffic rate; valid values are from 0 to 4294967 kbps.
infinity	Causes all sources for the specified group to use the shared tree.
group-list *access-list*	(Optional) Specifies the groups to which the threshold applies.

Command Default

When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If a source sends at a rate greater than or equal to the traffic rate (the *kbps* value), a PIM join message is triggered to construct a source tree.

The **group-list** *access-list* must be an IP standard access-list number or name. If the value is 0 or is omitted, the threshold applies to all groups.

If you specify the **infinity** keyword, all sources for the specified group use the shared tree. Specifying a group list access list indicates the groups to which the threshold applies.

If the traffic rate from the source drops below the threshold traffic rate, the leaf router will, after some amount of time, switch back to the shared tree and send a prune message to the source.

Examples

This example shows how to set a threshold of 4 kbps. If the traffic rate goes above this threshold, the traffic to a group from a source causes the router to switch to the shortest path tree to that source:

```
Router(config)# ip pim spt-threshold 4
Router(config)#
```

ip pim ssm

To define the SSM range of IP multicast addresses, use the **ip pim ssm** command. To disable the SSM range, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **ssm** {**default** | **range** *access-list*}

no ip pim [**vrf** *vrf-name*] **ssm**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
default	Defines the SSM range access list as 232/8.
range *access-list*	Specifies the standard IP access-list number or name defining the SSM range.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no MSDP source-active messages are accepted or originated in the SSM range.

Examples

This example shows how to configure the SSM service for the IP address range that is defined by access list 4:

```
access-list 4 permit 224.2.151.141
Router(config)# ip pim ssm range 4
```

Related Commands

Command	Description
ip igmp v3lite	Enables acceptance and processing of IGMP v3lite membership reports on an interface.
ip urd	Enables interception of TCP packets sent to the reserved URD port 465 on an interface and processing of URD channel subscription reports.

ip pim state-refresh disable

To disable the processing and forwarding of PIM dense-mode refresh-control messages on a PIM router, use the **ip pim state-refresh disable** command. To reenable the processing and forwarding of PIM dense-mode refresh-control messages, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **state-refresh disable**

no ip pim [**vrf** *vrf-name*] **state-refresh disable**

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.

Command Default

The processing and forwarding of PIM dense-mode refresh-control messages is enabled on PIM routers that are running a Cisco IOS software release that supports the PIM dense-mode refresh-control feature.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Configuring this command removes PIM dense-mode refresh-control information from PIM hello messages.

Examples

This example shows how to disable the periodic forwarding of the PIM dense-mode refresh-control message down a source-based IP multicast distribution tree:

```
Router(config)# ip pim state-refresh disable
Router(config)#
```

Related Commands

Command	Description
ip pim state-refresh origination-interval	Configures the origination of and the interval for PIM dense-mode state refresh-control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Displays the list that the PIM neighbors discovered.

ip rgmp

To enable RGMP on an interface, use the **ip rgmp** command. To disable RGMP, use the **no** form of this command.

ip rgmp

no ip rgmp

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are as follows:

- Enabled on Layer 2 interfaces (not configurable)
- Disabled on Layer 3 interfaces

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

These restrictions apply to RGMP on the PISA:

- You can enable RGMP on interfaces that are configured to support multicast routing.
- You must enable IGMP snooping on the Catalyst 6500 series switch.
- You must enable PIM on the Catalyst 6500 series switch.
- RGMP supports PIM sparse mode only. RGMP does not support PIM dense mode. RGMP explicitly supports the two AutoRP groups in dense mode by not restricting traffic to those groups but by flooding it to all router ports. For this reason, you should configure PIM sparse-dense mode. If you configure groups other than the AutoRP groups for dense mode, their traffic will not be correctly forwarded through router ports that have been enabled for RGMP.
- To effectively constrain multicast traffic with RGMP, connect RGMP-enabled routers to separate ports on RGMP-enabled Catalyst 6500 series switches.
- RGMP constrains only the traffic that exits through ports on which it detects an RGMP-enabled router. If a non-RGMP enabled router is detected on a port, that port receives all multicast traffic.
- RGMP does not support directly connected sources in the network. A directly connected source sends traffic into the network without signaling this information through RGMP or PIM. This traffic is not received by an RGMP-enabled router unless the router already requested receipt of that group through RGMP. This restriction applies to hosts and to functions in routers that source multicast traffic, such as the **ping** and **mtrace** commands, and multicast applications that source multicast traffic such as UDPTN.

- RGMP supports directly connected receivers in the network. Traffic to these receivers is restricted by IGMP snooping, or if the receiver is a router itself, by PIM and RGMP. CGMP is not supported in networks where RGMP is enabled on routers.
- Enabling RGMP and CGMP on a router interface is mutually exclusive. If RGMP is enabled on an interface, CGMP is silently disabled or vice versa.

Examples

This example shows how to enable RGMP:

```
Router(config-if)# ip rgmp
Router(config-if)#
```

This example shows how to disable RGMP:

```
Router(config-if)# no ip rgmp
Router(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

ip route-cache flow

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

ip route-cache flow

no ip route-cache flow

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

NetFlow switching captures a set of traffic statistics as part of its switching function. These traffic statistics include user, protocol, port, and type of service information that can be used for network analysis and planning, accounting, and billing. To export NetFlow data, use the **ip flow-export destination** or the **ip flow-export source** command in the global configuration mode.

NetFlow switching is supported on IP and IP-encapsulated traffic over all interface types and encapsulations except for ISL/VLAN, ATM, Frame Relay interfaces when more than one input access control list is used on the interface, and ATM LANE.

For additional information on NetFlow switching, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Note NetFlow does consume additional memory and CPU resources compared to other switching modes; we recommend that you understand the resources that are required on your router before you enable NetFlow.

Examples

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

```
Router(config-if)# ip route-cache flow
Router(config-if)#
```

This example shows how to return the interface to its defaults (fast switching enabled; autonomous switching disabled):

```
Router(config-if)# no ip route-cache flow
Router(config-if)#
```

Related Commands

Command	Description
ip flow-export destination	Exports the NetFlow cache entries to a specific destination.
show ip cache flow	Displays a summary of the NetFlow cache-flow entries.

ip sticky-arp (global configuration)

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

ip sticky-arp

no ip sticky-arp

Syntax Description

This command has no arguments or keywords.

Command Modes

Enabled

Command Default

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can enter the **ip sticky-arp (interface configuration)** command to disable sticky ARP on a specific interface.

ARP entries that are learned on Layer 3 interfaces are sticky ARP entries. We recommend that you display and verify ARP entries on the Layer 3 interface using the **show arp** command.

For security reasons, sticky ARP entries on the Layer 3 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 Layer 3 interface do not age out, you must manually remove ARP entries on the Layer 3 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:

```
Router(config) ip sticky-arp
Router(config)
```

This example shows how to disable sticky ARP:

```
Router(config) no ip sticky-arp
Router(config)
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (interface configuration)	Enables sticky ARP on an interface.
show arp	Displays the ARP table.

ip sticky-arp (interface configuration)

To enable sticky ARP on an interface, use the **ip sticky-arp** command. To remove the command, use the **no** form of this command.

ip sticky-arp [**ignore**]

no ip sticky-arp [**ignore**]

Syntax Description

ignore	(Optional) Overwrites the **ip sticky-arp (global configuration)** command.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can enter this command on any Layer 3 interface.

You can enter the **ip sticky-arp ignore** command to overwrite the PVLAN sticky-ARP global configuration on a specific interface.

Examples

This example shows how to enable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp
Router(config-if)
```

This example shows how to remove the previously configured command on an interface:

```
Router(config-if) no ip sticky-arp
Router(config-if)
```

This example shows how to disable sticky ARP on an interface:

```
Router(config-if) ip sticky-arp ignore
Router(config-if)
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.
ip sticky-arp (global configuration)	Enables sticky ARP.
show arp	Displays the ARP table.

ip unnumbered

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command. To disable IP processing on the interface, use the **no** form of this command.

ip unnumbered *interface-type number*

no ip unnumbered *interface-type number*

Syntax Description

interface-type number	Type and number of another interface on which the router has an assigned IP address; the interface cannot be another unnumbered interface.

Command Default

Disabled

Command Modes

Interface configuration (config-if) or Ethernet VLAN subinterfacem (config-subif)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The interface that you specify by the *interface-type number* arguments must be enabled (listed as “up” in the **show interfaces** command display).

The unnumbered interfaces and subinterfaces support peer IP address allocation through DHCP and have DHCP option 82 support.

The following restrictions apply when using IP unnumbering:

- You cannot enable IP unnumbering for a range of interfaces or subinterfaces that are configured through an interface or a subinterface range configuration.
- You cannot use the **ping** EXEC command to determine whether the interface is up, because the interface has no address. You can use SNMP to monitor the interface status remotely.
- You cannot boot a runnable image over an unnumbered serial interface.
- You cannot support IP security options on an unnumbered interface.

Examples

This example shows how to enable the IP unnumbered feature in the subinterface mode for Ethernet VLAN subinterfaces:

```
Router (config)# interface fastethernet1/0.1
Router (config-subif)# encapsulation dot1q 10
Router (config-subif)# ip unnumbered ethernet 3/0
```

This example shows how to disable the IP unnumbered feature for Ethernet physical interfaces:

```
Router (config)# interface fastethernet 1
Router (config-if)# no ip unnumbered loopback 0
Router (config-if)#
```

Related Commands

Command	Description
show ipv6 mld snooping explicit-tracking vlan	Displays MLDv2 snooping information.

ipv6 mfib-cef

To enable CEF-based (interrupt level) IPv6 multicast forwarding for outgoing packets on a specific interface, use the **ipv6 mfib-cef** command. To disable CEF-based IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib-cef

no ipv6 mfib-cef

Syntax Description

This command has no keywords or arguments.

Command Default

Enabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

CEF-based (interrupt level) IPv6 multicast forwarding is enabled by default when you enable CEF-based IPv6 multicast routing.

Use the **show ipv6 mfib interface** command to display the multicast forwarding interface status.

Examples

This example shows how to enable CEF-based IPv6 multicast forwarding:

```
Router(config-if) ipv6 mfib-cef
Router(config-if)
```

This example shows how to disable CEF-based IPv6 multicast forwarding:

```
Router(config-if) no ipv6 mfib-cef
Router(config-if)
```

Related Commands

Command	Description
show ipv6 mfib interface	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib hardware-switching

To configure hardware switching for IPv6 multicast packets on a global basis, use the **ipv6 mfib hardware-switching** command. To return to the default settings, use the **no** form of this command.

ipv6 mfib hardware-switching [**connected** | {**replication-mode ingress**}]

no ipv6 mfib hardware-switching [**connected** | {**replication-mode ingress**}]

Syntax Description

connected	(Optional) Allows you to download the interface and mask entry.
replication-mode ingress	(Optional) Sets the hardware replication mode to ingress.

Command Default

The defaults are as follows:

- **connected**—Enabled; installs subnet entries in the ACL-TCAM.
- **replication-mode**—Automatically detected; but can be forced to ingress.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can use the **ipv6 mfib hardware-switching** command for PIM SSM and PIM Bidir to prevent installation of the subnet entries on a global basis.

Examples

This example shows how to prevent the installation of the subnet entries on a global basis:

```
Router(config) ipv6 mfib hardware-switching
Router(config)
```

This example shows how to set the hardware replication mode to ingress:

```
Router(config) ipv6 mfib hardware-switching replication-mode
Router(config)
```

Related Commands

Command	Description
show platform software ipv6-multicast	Displays information about the platform software IPv6 multicast.

ipv6 mld snooping

To enable the MLDv2 snooping globally, use the **ipv6 mld snooping** command. To disable the MLDv2 snooping globally, use the **no** form of this command.

ipv6 mld snooping

no ipv6 mld snooping

Syntax Description

This command has no keywords or arguments.

Command Default

Enabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

Examples

This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
Router(config)#
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping explicit-tracking

To enable explicit host tracking, use the **ipv6 mld snooping explicit-tracking** command. To disable the explicit host tracking, use the **no** form of this command.

ipv6 mld snooping explicit-tracking

no ipv6 mld snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Explicit host tracking is supported only with MLDv2 hosts.

When you enable explicit host tracking and the Catalyst 6500 series switch is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Catalyst 6500 series switch forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With MLDv2 proxy reporting, the Catalyst 6500 series switch does proxy reporting for unsolicited reports and reports that are received in the general query interval.

Proxy reporting is turned on by default. When you disable proxy reporting, the Catalyst 6500 series switch works in transparent mode and updates the MLDv2 snooping database as it receives reports and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

MLDv2 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for MLDv2 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN, the MLDv2 snooping software processes the MLDv2 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that are reported by the host.
- The list of sources for each group that are reported by the hosts.
- The router filter mode of each group.
- The list of hosts for each group that request the source.

Examples

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping explicit-tracking
Router(config-if)#
```

Related Commands

Command	Description
ipv6 mld snooping limit	Configures the MLDv2 limits.
show ipv6 mld snooping explicit-tracking	Displays MLDv2 snooping information.

ipv6 mld snooping last-member-query-interval

To configure the last member query interval for MLDv2 snooping, use the **ipv6 mld snooping last-member-query-interval** command. To return to the default settings, use the **no** form of this command.

ipv6 mld snooping last-member-query-interval *interval*

no ipv6 mld snooping last-member-query-interval

Syntax Description

interval	Interval for the last member query; valid values are from 100 to 900 milliseconds in multiples of 100 milliseconds.

Command Default

1000 milliseconds (1 second); see the "Usage Guidelines" section for additional information.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When a multicast host leaves a group, the host sends an MLDv2 leave. To check if this host is the last to leave the group, an MLDv2 query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Catalyst 6500 series switch waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable MLDv2 fast-leave processing and you enter the **no ipv6 mld snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes a higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of **1000**. If you want this value, you must enter the **no ipv6 mld snooping last-member-query-interval** command and return to the default value (1000 milliseconds).

Examples

This example shows how to configure the last-member-query-interval to 200 milliseconds:

```
Router(config-if)# ipv6 mld snooping last-member-query-interval 200
Router(config-if)#
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping limit

To configure the MLDv2 limits, use the **ipv6 mld snooping limit** command. To return to the default settings, use the **no** form of this command.

ipv6 mld snooping limit {{**l2-entry-limit** *max-entries*} | {**rate** *pps*} | {**track** *max-entries*}}

no ipv6 mld snooping limit {**l2-entry-limit** | **rate** | **track**}

Syntax Description

l2-entry-limit *max-entries*	Specifies the maximum number of Layer 2 entries that can be installed by MLD snooping; valid values are from 1 to 100000 entries.
rate *pps*	Specifies the rate limit of incoming MLDv2 messages; valid values are from 100 to 6000 packets per second.
track *max-entries*	Specifies the maximum number of entries in the explicit-tracking database; valid values are from 0 to 128000 entries.

Command Modes

max-entries is **32000**.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.

When you set the *max-entries* to **0**, explicit-tracking is disabled.

When the explicit-tracking database exceeds the configured *max-entries*, a syslog message is generated.

When you reduce the *max-entries*, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

Examples

This example shows how to set the maximum number of Layer 2 entries that can be installed by MLD snooping:

```
Router(config)# ipv6 mld snooping limit l2-entry-limit 20000
Router(config)#
```

This example shows how to set the rate limit for incoming MLDv2-snooping packets:

```
Router(config)# ipv6 mld snooping limit rate 200
Router(config)#
```

This example shows how to configure the maximum number of entries in the explicit-tracking database:

```
Router(config)# ipv6 mld snooping limit track 20000
Router(config)#
```

This example shows how to disable software rate limiting:

```
Router(config)# no ipv6 mld snooping limit rate
Router(config)#
```

Related Commands

Command	Description
ipv6 mld snooping explicit-tracking	Enables explicit host tracking.
show ipv6 mld snooping	Displays the information about the snooping status for MLDv2 hosts.

ipv6 mld snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ipv6 mld snooping mrouter** command.

ipv6 mld snooping mrouter {**interface** *type slot/port*}

Syntax Description

interface *type*	Specifies the interface type: valid values are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
slot/ports	Module and port number.

Command Default

None configured

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

To configure a static connection to a multicast router, use the **mac-address-table static** command.

Examples

This example shows how to configure a Layer 2 port as a multicast router port:

```
Router(config-if)# ipv6 mld snooping mrouter interface fastethernet 5/6
Router(config-if)#
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping querier

To enable the MLDv2 snooping querier, use the **ipv6 mld snooping querier** command. To disable the MLDv2 snooping querier, use the **no** form of this command.

ipv6 mld snooping querier

no ipv6 mld snooping querier

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Configure an IPv6 address on the VLAN interface. When enabled, the MLDv2 snooping querier uses the IPv6 address as the query source address.

If there is no IPv6 address configured on the VLAN interface, the MLDv2 snooping querier does not start. The MLDv2 snooping querier disables itself if the IPv6 address is cleared. When enabled, the MLDv2 snooping querier restarts if you configure an IPv6 address.

When enabled, the MLDv2 snooping querier does not start if it detects MLDv2 traffic from an IPv6 multicast router.

When enabled, the MLDv2 snooping querier starts after 60 seconds if it detects no MLDv2 traffic from an IPv6 multicast router.

When enabled, the MLDv2 snooping querier disables itself if it detects MLDv2 traffic from an IPv6 multicast router.

You can enable the MLDv2 snooping querier on all the Catalyst 6500 series switches in the VLAN that support it. One switch is elected as the querier.

Examples

This example shows how to enable the MLDv2 snooping querier on VLAN 200:

```
Router# interface vlan 200
Router(config-if)# ipv6 mld snooping querier
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping report-suppression

To enable report suppression on a VLAN, use the **ipv6 mld snooping report-suppression** command. To disable report suppression on a VLAN, use the **no** form of this command.

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Syntax Description

This command has no keywords or arguments.

Command Default

Enabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must enable explicit tracking before enabling report suppression.

This command is supported on VLAN interfaces only.

Examples

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping report-suppression
Router(config-if)#
```

ip verify unicast reverse-path

To enable unicast RPF, use the **ip verify unicast reverse-path** command. To disable unicast RPF, use the **no** form of this command.

ip verify unicast reverse-path [**allow-self-ping**] [*list*]

no ip verify unicast reverse-path [**allow-self-ping**] [*list*]

Syntax Description

allow-self-ping	(Optional) Allows the Catalyst 6500 series switch to ping itself.
list	(Optional) Access-list number; valid values are from 1 to 199 for a standard or extended IP access-list number and from 1300 to 2699 for a standard or extended IP expanded access-list number.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use the **ip verify unicast reverse-path** command to mitigate problems that are caused by malformed or forged (spoofed) IP source addresses that pass through a Catalyst 6500 series switch. Malformed or forged source addresses can indicate DoS attacks that are based on source IP address spoofing.

Note Unicast RPF is an input function and is applied only on the input interface of a Catalyst 6500 series switch at the upstream end of a connection.

If you do not specify an ACL in the **ip verify unicast reverse-path** command, the Catalyst 6500 series switch drops the forged or malformed packet immediately and no ACL logging occurs. The Catalyst 6500 series switch and interface unicast RPF counters are updated.

You can log unicast RPF events by specifying the logging option for the ACL entries that are used by the **ip verify unicast reverse-path** command. You can use the logging option to gather information about the attack, such as the source address, time, and so on.

Note With unicast RPF, all equal-cost “best” return paths are considered valid. Unicast RPF works when multiple return paths exist, if each path is equal to the others in the routing cost (such as the number of hops, weights, and so on), and the route is in the FIB. Unicast RPF also functions where EIGRP variants are used and unequal candidate paths that go back to the source IP address exist.

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

Routers at the edge of a service-provider network are more likely to have symmetrical reverse paths than routers that are in the core of the network. Routers that are in the core of the service-provider network have no guarantee that the best forwarding path out of the router is the path that is selected for packets returning to the router.

We do not recommend that you apply unicast RPF where there is a chance of asymmetric routing. You should place unicast RPF only at the edge of a network. In a service-provider network, you should place the unicast RPF at the customer edge of the network.

Examples

This example shows how to enable unicast RPF on a serial interface:

```
Router(config-if)# ip verify unicast reverse-path
Router(config-if)#
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor.

ip verify unicast source reachable-via

To enable and configure RPF checks, use the **ip verify unicast source reachable-via** command. To disable RPF, use the **no** form of this command.

ip verify unicast source reachable-via {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*list*]

no ip verify unicast source reachable-via

Syntax Description

rx	Checks that the source address is reachable on the interface where the packet was received.
any	Checks that the source address is reachable on any path.
allow-default	(Optional) Checks that the default route matches the source address.
allow-self-ping	(Optional) Allows the router to ping itself.
list	(Optional) Access-list number; valid values are from 1 to 199 for a standard IP access-list number and from 1300 to 2699 for a standard IP expanded access-list number.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Unicast RPF is not supported on PVLAN host ports.

Unicast RPF provides three basic modes:

- Exists-only mode—A source address needs to be present only in the FIB and reachable through a “real” interface; this situation also applies to the **ip verify unicast source reachable-via any allow-default** command. The exists-only mode requires that a resolved and reachable source address is present in the FIB table. The source address must be reachable through a configured interface.
- Any mode—The source must be reachable through any of the paths. For example, the source has per-destination load balancing.
- Rx mode—A source address must be reachable on the arrived interface. For example, the source must be reachable without load balancing.

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

When configuring uRPF check, use the following guidelines and restrictions:

- If you configure uRPF check to filter with an ACL, the PFC determines whether or not traffic matches the ACL. The PFC sends the traffic denied by the RPF ACL to the PISA for the uRPF check. Packets permitted by the ACL are forwarded in hardware without a uRPF check. You can enter the **mls ip cef rpf hw-enable-rpf-acl** command to subject to RPF check and forwarding in hardware and the Packets that are denied by the uRPF ACL are forwarded in hardware and the packets that are permitted by ACL are sent to software.
- Because the packets in a DoS attack typically match the deny ACE and are sent to the PISA for the uRPF check, they can overload the PISA. You can enter the **mls ip cef rpf hw-enable-rpf-acl** command in these cases since DOS packets matching the deny ACE are processed in hardware.

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

Examples

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

```
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)#
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor.
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

ip wccp group-listen

To enable the reception of IP multicast packets for WCCP, use the **ip wccp group-listen** command mode. To disable the reception of IP multicast packets for WCCP, use the **no** form of this command.

ip wccp {**web-cache** | {*service-number* | *service-name*}} **group-listen**

no ip wccp {**web-cache** | {*service-number* | *service-name*}} **group-listen**

Syntax Description

web-cache	Directs the router to send packets to the web cache service.
service-number	WCCP service number; valid values are from 0 to 99.
service-name	WCCP service name; the valid value is **web-cache**.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Note To ensure that the command operates correctly, you must enter the **ip pim** *mode* command in addition to the **ip wccp group-listen** command.

The *service-number* may be either **web-cache** or a number representing a cache engine dynamically defined definition. Once the service is enabled, the Catalyst 6500 series switch can participate in the establishment of a service group.

On Catalyst 6500 series switches that are to be members of a service group when IP multicast is used, the following configuration is required:

- You must configure the IP multicast address for use by the WCCP service group.
- You must configure the **ip wccp** {**web-cache** | *service-number*} **group-listen** command on the interfaces that are to receive the IP multicast address.

Examples

This example shows how to enable the multicast packets for a web cache with a multicast address of 224.1.1.100:

```
router# configure terminal
router(config)# ip wccp web-cache group-address 244.1.1.100
router(config)# interface ethernet 0
router(config-if)# ip wccp web-cache group-listen
```

Related Commands

Command	Description
ip wccp	Directs a router to enable or disable the support for a cache engine service group.
ip wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.

ip wccp redirect

To enable packet redirection on an outbound or inbound interface using WCCP, use the **ip wccp redirect** command. To disable WCCP redirection, use the **no** form of this command

ip wccp {**web-cache** | *service-number*} **redirect** {**in** | **out**}

no ip wccp {**web-cache** | *service-number*} **redirect** {**in** | **out**}

Syntax Description

web-cache	Enables the web-cache service.
service-number	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 99. If Cisco cache engines are used in the cache cluster, the **reverse proxy** service is indicated by a value of 99.
redirect	Enables packet redirection checking on an outbound or inbound interface.
in	Specifies packet redirection on an inbound interface.
out	Specifies packet redirection on an outbound interface.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **ip wccp redirect in** command allows you to configure WCCP redirection on an interface that receives inbound network traffic. When the command is applied to an interface, all packets that arrive at that interface are compared with the criteria that is defined by the specified WCCP service. If the packets match the criteria, they are redirected.

The **ip wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.

Note This command can affect the **ip wccp redirect exclude in** command. If you have the **ip wccp redirect exclude in** command set on an interface and you configure the **ip wccp redirect in** command, the **ip wccp redirect exclude in** command is overridden. The opposite is also true: configuring the **ip wccp redirect exclude in** command overrides the **ip wccp redirect in** command.

For a complete description of the WCCP configuration commands, including a list of commands that have changed since Cisco IOS Release 12.0, refer to the “WCCP Commands” chapter in the “Cisco IOS System Management Commands” part of the *Cisco IOS Release 12.2 Command Reference*.

Examples

This example shows how to configure a session in which the reverse proxy packets on the Ethernet interface 0 are checked for redirection and are redirected to a Cisco cache engine:

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

This example shows how to configure a session in which the HTTP traffic that arrives on interface 0/1 is redirected to a Cisco cache engine:

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces that are configured for IP.
show ip wccp	Displays the WCCP statistics.

ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command. To disable hardware acceleration, use the **no** form of this command.

ip wccp web-cache accelerated {[**group-address** *groupaddress*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]}

no ip wccp web-cache accelerated

Syntax Description

group-address *groupaddress*	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the "Usage Guidelines" section for additional information.
redirect-list *access-list*	(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the "Usage Guidelines" section for additional information.
group-list *access-list*	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the "Usage Guidelines" section for additional information.
password *password*	(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the "Usage Guidelines" section for additional information.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on software releases later than cache engine software Release ACNS 4.2.1.

The **group-address** *groupaddress* option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages that it has received on this group address. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all "Here I Am" messages are responded to with a unicast reply.

The **redirect-list** *access-list* option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or extended access-list number or a name to represent a named standard or extended access list. The access list specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **group-list** *access-list* option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access-list number or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

Examples

This example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
Router(config)#
```

Related Commands

Command	Description
ip wccp version	Specifies which version of WCCP to configure on your router.

l2protocol-tunnel

To enable the protocol tunneling on an interface and specify the type of protocol to be tunneled, use the **l2protocol-tunnel** command. To disable protocol tunneling, use the **no** form of this command.

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

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

Syntax Description

cdp	(Optional) Enables CDP tunneling.
stp	(Optional) Enables STP tunneling.
vtp	(Optional) Enables VTP tunneling.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

On all the service provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

Note PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, all protocols are tunneled.

You can configure protocol tunneling on VLAN and trunk interfaces.

You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Examples

This example shows how to enable a tunneling protocol on an interface:

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

This example shows how to disable a tunneling protocol on an interface:

```
Router(config-if)# no l2protocol-tunnel
Protocol tunneling disabled on interface fastEthernet 4/1
Router(config-if)#
```

Related Commands

Command	Description
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.

l2protocol-tunnel cos

To specify a CoS value globally on all ingress Layer-2 protocol tunneling ports, use the **l2protocol-tunnel cos** command. To return to the default settings, use the **no** form of this command.

l2protocol-tunnel cos *cos-value*

no l2protocol-tunnel cos

Syntax Description

cos-value	CoS value; valid values are from 0 to 7.

Command Default

The *cos-value* is **5**.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The *cos-value* is the CoS value that you assign to the PDUs on a Layer 2-protocol tunnel port before tunneling the PDUs through the service-provider network.

You can specify a CoS value globally on all ingress Layer 2-protocol tunneling ports. Because the CoS value applies to all ingress tunneling ports, all encapsulated PDUs that are sent out by the Catalyst 6500 series switch have the same CoS value.

On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

Note PortFast BPDU filtering is enabled automatically on tunnel ports.

Examples

This example shows how to specify a CoS value on all ingress Layer 2-protocol tunneling ports:

```
Router(config)# l2protocol-tunnel cos 6
Router(config)#
```

Related Commands

Command	Description
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.

l2protocol-tunnel drop-threshold

To specify the maximum number of packets that can be processed for the specified protocol on that interface before being dropped, use the **l2protocol-tunnel drop-threshold** command. To reset all the threshold values to 0 and disable the drop threshold, use the **no** form of this command.

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

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

Syntax Description

cdp	(Optional) Specifies CDP packets.
stp	(Optional) Specifies STP packets.
vtp	(Optional) Specifies VTP packets.
packets	Maximum number of packets; valid values are from 1 to 4096 packets.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

Note PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, the threshold applies to all protocols.

You can configure protocol tunneling on switch ports only. You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Refer to the "Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling" chapter of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional information on setting the drop threshold value.

Examples

This example shows how to set the drop threshold:

```
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel drop-threshold 3000
Router(config-if)#
```

Related Commands

Command	Description
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
l2protocol-tunnel cos	Specifies a CoS value globally on all ingress Layer-2 protocol tunneling ports.
l2protocol-tunnel global drop-threshold	Enables rate limiting at the software level.
l2protocol-tunnel shutdown-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.

l2protocol-tunnel global drop-threshold

To enable rate limiting at the software level, use the **l2protocol-tunnel global drop-threshold** command. To disable the software rate limiter on the Catalyst 6500 series switch, use the **no** form of this command.

l2protocol-tunnel global drop-threshold *threshold*

no l2protocol-tunnel global drop-threshold

Syntax Description

threshold	Maximum rate of incoming PDUs before excessive PDUs are dropped; valid values are from 100 to 20000 PDUs.

Command Default

Global thresholds are not configured.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

All three PDUs (normal BPDU, CDP, and VTP packets) that arrive on Layer 2-protocol tunnel-enabled ports are rate limited. Rate limiting occurs in the ingress direction in Layer 2-protocol tunneling. If the rate of the incoming PDUs exceeds the configured *threshold*, the excessive PDUs are dropped.

Examples

This example shows how to enable rate limiting globally:

```
Router(config)# l2protocol-tunnel global drop-threshold 3000
Router(config)#
```

Related Commands

Command	Description
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
l2protocol-tunnel cos	Specifies a CoS value globally on all ingress Layer-2 protocol tunneling ports.
l2protocol-tunnel drop-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface before being dropped.
l2protocol-tunnel shutdown-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.

l2protocol-tunnel shutdown-threshold

To specify the maximum number of packets that can be processed for the specified protocol on that interface in 1 second, use the **l2protocol-tunnel shutdown-threshold** command. To reset all the threshold values to 0 and disable the shutdown threshold, use the **no** form of this command.

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

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

Syntax Description

cdp	(Optional) Specifies CDP tunneling.
stp	(Optional) Specifies STP tunneling.
vtp	(Optional) Specifies VTP tunneling.
packets	Shutdown threshold; valid values are from 1 to 4096.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When the number of *packets* is exceeded, the port is put in error-disabled state.

On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

Note PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, the *packets* value applies to all protocols.

You can configure protocol tunneling on switch ports only. You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Refer to the "Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling" chapter of the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional information on setting the drop threshold value.

Examples

This example shows how to specify the maximum number of CDP packets that can be processed on that interface in 1 second:

```
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 200
Router(config-if)#
```

Related Commands

Command	Description
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.

l2 vfi manual

To create a Layer 2 VFI and enter the Layer 2 VFI manual configuration submode, use the **l2 vfi manual** command. To remove the Layer 2 VFI, use the **no** form of this command.

l2 vfi *name* **manual**

no l2 vfi *name* **manual**

Syntax Description

name	Name of a new or existing Layer 2 VFI.

Command Default

This command has no default settings.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

A VFI is a collection of data structures used by the data plane, software-based or hardware-based, to forward packets to one or more VCs. It is populated and updated by both the control plane and the data plane and also serves as the data structure interface between the control plane and the data plane.

Within the Layer 2 VFI manual configuration submode, you can configure the following parameters:

- VPN ID of a VPLS domain
- Addresses of other PE routers in this domain
- Type of tunnel signaling and encapsulation mechanism for each peer

Within the Layer 2 VFI manual configuration submode, the following commands are available:

- [**no**] **vpn id** *vpn-id*—Configures a VPN ID in RFC 2685 format. To remove the VPN ID from the configuration, use the **no** form of this command.
- [**no**] **neighbor** *remote-router-id* {**encapsulation** {**l2tpv3** | **mpls**} | {**pw-class** *pw-name*} | **no-split-horizon**}—Specifies the type of tunnel signaling and encapsulation mechanism for each peer. See the **neighbor** command.

Examples

This example shows how to create a Layer 2 VFI, enter the Layer 2 VFI manual configuration submode, and configure a VPN ID:

```
Router(config)# l2 vfi vfitest1 manual
Router(config-vfi)# vpn id 303
```

lacp max-bundle

To define the maximum number of bundled LACP ports allowed in this port channel, use the **lacp max-bundle** command. To return to the default settings, use the **no** form of this command.

lacp max-bundle *max-bundles*

no lacp max-bundle

Syntax Description

max-bundles	Maximum number of bundled ports allowed in this port channel; valid values are from 1 to 8.

Command Default

The default settings are as follows:

- Maximum of eight bundled ports.
- Maximum of eight bundled ports and eight hot-standby ports per port channel; this setting applies if the port channel on both sides of the LACP bundle are configured the same.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to set the maximum number of ports to bundle in this port channel:

```
Router(config-if)# lacp max-bundle 4
Router(config-if)#
```

Related Commands

Command	Description
show lacp	Displays LACP information.

lacp port-priority

To set the 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.

Command Default

32768

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must assign a port priority to each port in the Catalyst 6500 series switch. You can specify the port priority 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, *priority* is supported only on port channels with LACP-enabled physical interfaces.

This command is supported on LACP-enabled interfaces.

When setting the priority, note that a higher number means a lower priority.

Examples

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

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

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
channel-protocol	Sets the protocol that is used on an interface to manage channeling.
lacp system-priority	Sets the priority of the system.
show lacp	Displays LACP information.

lacp rate

To set the rate at which the LACP packets are ingressed to an interface, use the **lacp rate** command. To return to the default settings, use the **no** form of this command.

lacp rate {**normal** | **fast**}

no lacp rate

Syntax Description

normal	Specifies that the LACP packets are ingressed at the normal rate of 30-seconds rate.
fast	Specifies that the LACP packets are ingressed at the fast rate of 1-second rate once the link is established.

Command Default

90 seconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on LACP-enabled interfaces.

Examples

This example shows how to specify that the LACP packets are ingressed at the one-second rate:

```
Router(config-if)# lacp rate fast
Router(config-if)#
```

Related Commands

Command	Description
show lacp	Displays LACP information.

lacp system-priority

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

lacp system-priority *priority*

Syntax Description

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

Command Default

32768

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You must assign a system priority to each Catalyst 6500 series switch running LACP. You can specify the system priority automatically or by entering the **lacp system-priority** command. The system priority is used with the Catalyst 6500 series 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, *priority* is supported on port channels with LACP-enabled physical interfaces.

When setting the priority, note that a higher number means a lower priority.

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

Examples

This example shows how to set the system priority:

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

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
channel-protocol	Sets the protocol that is used on an interface to manage channeling.
lacp port-priority	Sets the priority for the physical interfaces.
show lacp	Displays LACP information.

line

To identify a specific line for configuration and enter line configuration collection mode, use the **line** command.

line {{*first-line-number* [*ending-line-number*]} | {**console** *first-line-number*} | {**vty** {*first-line-number* [*ending-line-number*]}}}

Syntax Description

first-line-number	Relative number of the terminal line (or the first line in a contiguous group) that you want to configure when the line type is specified; valid values are from 0 to 1510.
ending-line-number	(Optional) Relative number of the last line in a contiguous group that you want to configure; valid values are from 101 to 1510.
console *first-line-number*	Specifies the console terminal line; the valid value is **0**.
vty	Specifies the virtual terminal line for remote console access.

Command Default

This command has no default settings.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The console port is DCE.

If you do not specify **console** or **vty**, the *first-line-number* and *ending-line-number* are absolute rather than relative line numbers.

You can address a single line or a consecutive range of lines with the **line** command. A line number is necessary, though, and you will receive an error message if you forget to include it.

Entering the **line** command with the optional line type (**console** or **vty**) designates the line number as a relative line number. For example, to configure line parameters for line 7 (a TTY line), you could enter the **line tty 7** command.

You also can use the **line** command without specifying a line type. In this case, the line number is treated as an absolute line number. For example, to configure line parameters for line 5, which can be of any type, you could enter the **line 5** command.

Absolute line numbers increment consecutively and can be difficult to manage on large systems. Relative line numbers are a shorthand notation used in configurations. Internally, the Cisco IOS software uses absolute line numbers. You cannot use relative line numbers everywhere, but you can use absolute line numbers everywhere.

You can enter the **show users all** command to display a table of absolute and relative line numbers. The absolute line numbers are listed at the far left, followed by the line type, and then the relative line number. Relative line numbers always begin at zero and define the type of line. Addressing the second virtual terminal line as line VTY 1, for example, is easier than remembering it as line 143—its absolute line number.

The terminal from which you locally configure the router is attached to the console port. To configure line parameters for the console port, enter the **line console 0** command. The console relative line number must be **0**.

Once you enter the line console configuration mode, you can set the transmit and receive speeds; valid values are from 0 to 9600. The default rate is 9600.

Virtual terminal lines are used to allow remote access to the router. A virtual terminal line is not associated with either the auxiliary or console port. The router has five virtual terminal lines by default. However, you can create additional virtual terminal lines as described in the chapter "Configuring Protocol Translation and Virtual Asynchronous Devices" in the *Cisco IOS Terminal Services Configuration Guide*.

Configuring the console port or virtual terminal lines allows you to perform such tasks as setting communication parameters, specifying autobaud connections, and configuring terminal operating parameters for the terminal that you are using.

Examples

This example shows how to start the configuration for virtual terminal lines 0 to 4:

```
Router(config)# line vty 0 4
Router(config-line)#
```

This example shows how to create and configure the maximum 100 virtual terminal lines with the **no login** command:

```
Router(config)# line vty 0 99
Router(config-line)# no login
Router(config-line)#
```

This example shows how to eliminate the virtual terminal line number 5 and all higher-numbered virtual terminal lines. Only virtual terminal lines 0 to 4 will remain.

```
Router(config-line)# no line vty 5
Router(config)#
```

This example shows how to set the transmit and receive speeds for the console port:

```
Router(config)# line console 0
Router(config-line)# speed 9600
Router(config-line)#
```

Related Commands

Command	Description
show line	Displays parameters of a terminal line.
show users	Displays information about the active lines on the router.

link debounce

To enable the debounce timer on an interface, use the **link debounce** command. To disable the timer, use the **no** form of this command.

link debounce [**time** *time*]

no link debounce

Syntax Description

time *time*	(Optional) Specifies the extended debounce timer; valid values are from 100 to 5000 milliseconds.

Command Default

Table 2-13 lists the debounce timer defaults.

Table 2-13 Port Debounce Timer Delay Time

Port Type	Debounce Timer Disabled	Debounce Timer Enabled
10BASE-FL ports	300 milliseconds	3100 milliseconds
10/100BASE-TX ports	300 milliseconds	3100 milliseconds
100BASE-FX ports	300 milliseconds	3100 milliseconds
10/100/1000BASE-TX ports	300 milliseconds	3100 milliseconds
1000BASE-TX ports	300 milliseconds	3100 milliseconds
Fiber Gigabit ports	10 milliseconds	100 milliseconds
10-Gigabit ports except WS-X6501-10GEX4 and WS-X6502-10GE	10 milliseconds	100 milliseconds
WS-X6501-10GEX4 and WS-X6502-10GE 10-Gigabit ports	1000 milliseconds	3100 milliseconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **time** *time* keyword and argument are supported on Gigabit Ethernet and 10-Gigabit Ethernet interfaces only.

The **time** *time* keyword and argument are not supported on copper media.

The debounce timer sets the amount of time that the firmware waits before it notifies the software that the link is down. The debounce timer does not apply to linkup because the linkup is immediately notified by the firmware.

The default debounce time applies when you enter the **link debounce** command with no arguments. For example, when you enter the **link debounce time 100** command, it is equivalent to entering the **link debounce** command with no arguments. You will see the following link debounce entry in the configuration:

```
interface GigabitEthernet1/1
 no ip address
 link debounce
```

Enter the **show interfaces debounce** command to display the debounce configuration of an interface.

Examples

This example shows how to configure the debounce timer on a Gigabit Ethernet fiber interface:

```
Router (config-if)# link debounce time 100
Router (config-if)#
```

Related Commands

Command	Description
show interfaces debounce	Displays the status and configuration for the debounce timer.

load-interval

To specify the length of time to be used to calculate the average load for an interface, use the **load-interval** command. To return to the default settings, use the **no** form of this command.

load-interval *seconds*

no load-interval

Syntax Description

seconds	Length of time that is used to compute load statistics; valid values are from 30 to 600 seconds in 30-second increments.

Command Default

300 seconds (5 minutes)

Command Modes

Interface configuration (config-if)
Frame Relay DLCI configuration (config-fr-dlci)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

By default, the load data is gathered every 5 minutes or 300 seconds. You can use this data to compute load statistics, including the input rate in bits and packets per second, and the output rate in bits and packets per second, load, and reliability. Load data is computed using a weighted-average calculation where recent load data has more weight than older load data.

If you want the load computations to be more reactive to short bursts of traffic, rather than being averaged over 5-minute periods, you can shorten the length of time over which load averages are computed. For example, you can set the load interval to 30 seconds to reflect the weighted-average load for the last 30-second period.

Enter the **load-interval** command to change the calculation interval from the default value of 5 minutes (300 seconds) to a shorter or longer period of time. If you change it to a shorter period of time, the input and output statistics that are displayed when you use the **show interface** or **show frame-relay pvc** command will be more current, rather than reflecting a more average load over a longer period of time.

Enter the **load-interval** command to increase or decrease the likelihood of activating a backup interface; for example, a backup dial interface may be triggered by a sudden spike in the load on an active interface.

Examples

This example shows how to set the load interval for the serial interface 0 so that the average is computed over 30-second intervals:

```
Router(config)# interface serial 0
Router(config-if)# load-interval 30
```

This example shows how to set the load interval to 60 seconds for a Frame Relay PVC with the DLCI 100:

```
Router(config)# interface serial 1/1
Router(config-if# encapsulation frame-relay ietf
Router(config-if)# frame-relay interface-dlci 100
Router(config-fr-dlci)# load-interval 60
```

Related Commands

Command	Description
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.

logging event link-status (global configuration)

To change the default or set the link-status event messaging during system initialization, use the **logging event link-status** command. To disable the link-status event messaging, use the **no** form of this command.

logging event link-status {**default** | **boot**}

no logging event link-status {**default** | **boot**}

Syntax Description

default	Enables system logging of interface state-change events on all interfaces in the system.
boot	Enables system logging of interface state-change events on all interfaces in the system during system initialization.

Command Default

Interface state-change messages are not sent.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You do not have to enter the **logging event link-status boot** command to enable link-status messaging during system initialization. The **logging event link-status default** command logs system messages even during system initialization.

If you enter both the **logging event link-status default** and the **no logging event link-status boot** commands, the interface state-change events are logged after all modules in the Catalyst 6500 series switch come online after system initialization. The **logging event link-status default** and the **no logging event link-status boot** commands are saved and retained in the running configuration of the system.

When both the **logging event link-status default** and the **no logging event link-status boot** commands are present in the running configuration and you want to display the interface state-change messages during system initialization, enter the **logging event link-status boot** command.

Examples

This example shows how to enable the system logging of the interface state-change events on all interfaces in the system:

```
Router(config)# logging event link-status default
Router(config)#
```

This example shows how to enable the system logging of interface state-change events on all interfaces during system initialization:

```
Router(config)# logging event link-status boot
Router(config)#
```

This example shows how to disable the system logging of interface state-change events on all interfaces:

```
Router(config)# no logging event link-status default
Router(config)#
```

This example shows how to disable the system logging of interface state-change events during system initialization:

```
Router(config)# no logging event link-status boot
Router(config)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

logging event link-status (interface configuration)

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

logging event link-status

no logging event link-status

Syntax Description

This command has no arguments or keywords.

Command Default

Interface state-change messages are not sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event link-status** command.

Examples

This example shows how to enable the system logging of the interface state-change events on an interface:

```
Router(config-if)# logging event link-status
Router(config-if)#
```

This example shows how to disable the system logging of the interface state-change events on an interface:

```
Router(config-if)# no logging event link-status default
Router(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

logging event subif-link-status

To enable the link-status event messaging on a subinterface, use the **logging event subif-link-status** command. To disable the link-status event messaging on a subinterface, use the **no** form of this command.

logging event subif-link-status

no logging event subif-link-status

Syntax Description

This command has no arguments or keywords.

Command Default

Subinterface state-change messages are not sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on the following subinterfaces:

- Frame Relay subinterfaces
- OSM-GE-WAN subinterfaces
- SIP subinterfaces
- LAN subinterfaces

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

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

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event link-status** command.

Examples

This example shows how to enable the system logging of the interface state-change events on a subinterface:

```
Router(config-if)# logging event subif-link-status
Router(config-if)#
```

This example shows how to disable the system logging of the interface state-change events on a subinterface:

```
Router(config-if)# no logging event subif-link-status
Router(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

logging ip access-list cache (global configuration mode)

To configure the OAL parameters, use the **logging ip access-list cache** command. To return to the default settings, use the **no** form of this command.

logging ip access-list cache {{**entries** *entries*} | {**interval** *seconds*} | {**rate-limit** *pps*} | {**threshold** *packets*}}

no logging ip access-list cache [**entries** | **interval** | **rate-limit** | **threshold**]

Syntax Description

entries *entries*	Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries.
interval *seconds*	Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds.
rate-limit *pps*	Specifies the number of packets that are logged per second in the software; valid values are from 10 to 1000000 pps.
threshold *packets*	Specifies the number of packet matches before an entry is sent to syslog; valid values are from 1 to 1000000 packets.

Command Default

The defaults are as follows:

- *entries*—**8000** entries.
- *seconds*—**300** seconds (5 minutes).
- **rate-limit** *pps*—**0** (rate limiting is off) and all packets are logged.
- **threshold** *packets*—**0** (rate limiting is off) and the system log is not triggered by the number of packet matches.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, the entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

Examples

This example shows how to specify the maximum number of log entries that are cached in the software:

```
Router(config)# logging ip access-list cache entries 200
Router(config)#
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
Router(config)# logging ip access-list cache interval 350
Router(config)#
```

This example shows how to specify the number of packets that are logged per second in the software:

```
Router(config)# logging ip access-list cache rate-limit 100
Router(config)#
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
Router(config)# logging ip access-list cache threshold 125
Router(config)#
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (interface configuration mode)	Enables an OAL-logging cache on an interface that is based on direction.
show logging ip access-list	Displays information about the logging IP access list.

logging ip access-list cache (interface configuration mode)

To enable an OAL-logging cache on an interface that is based on direction, use the **logging ip access-list cache** command. To disable OAL, use the **no** form of this command.

logging ip access-list cache [**in** | **out**]

no logging ip access-list cache

Syntax Description

in	(Optional) Enables OAL on ingress packets.
out	(Optional) Enables OAL on egress packets.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on traffic that matches the **log** keyword in the applied ACL. You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

On systems that are configured with a PFC3A, support for the egress direction on tunnel interfaces is not supported.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, the entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

Examples

This example shows how to enable OAL on ingress packets:

```
Router(config-if)# logging ip access-list cache in
Router(config-if)#
```

This example shows how to enable OAL on egress packets:

```
Router(config-if)# logging ip access-list cache out
Router(config-if)#
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration mode)	Configures the OAL parameters.
show logging ip access-list	Displays information about the logging IP access list.

mac access-list extended

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

mac access-list extended *name*

no mac access-list extended *name*

Syntax Description

name	Name of the ACL to which the entry belongs.

Command Default

No default ACL

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

- Maximum of 31 characters and may 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**

You can configure named ACLs that filter IPX, DECnet, AppleTalk, VINES, or XNS traffic based on MAC addresses (IPX filtering with a MAC ACL is supported only with a PFC3).

In systems that are configured with PFC3, if you want to classify all IPX traffic by using a MAC-access list that matches on EtherType 0x8137, use the **ipx-arpa** or **ipx-non-arpa** protocol.

Once you enter the **mac access-list extended** *name* command, use the following subset to create or delete entries in a MAC-access list:

[**no**] {**permit** | **deny**} {{*src-mac mask* | **any**} {*dest-mac mask*} | **any**} [*protocol* [**vlan** *vlan*] [**cos** *value*]]

The **vlan** *vlan* and **cos** *value* keywords and arguments are supported in PFC3BXL or PFC3B mode.

The **vlan** *vlan* and **cos** *value* keywords and arguments are not supported on the MAC VACLs.

Table 2-14 describes the syntax of the **mac access-list extended** subcommands.

Table 2-14 mac access-list extended Subcommands

Subcommand	Description
no	(Optional) Deletes a statement from an access list.
permit	Permits access if the conditions are matched.
deny	Denies 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.
dest-mac mask	(Optional) Destination MAC address in the form: *dest-mac-address dest-mac-address-mask*.
protocol	(Optional) Name or number of the protocol; see below for a list of valid values.
vlan *vlan*	(Optional) Specifies a VLAN ID; valid values are from 0 to 4095.
cos *value*	(Optional) Specifies a CoS value; valid values are from 0 to 7.

Valid protocol names are as follows:

- 0x0-0xFFFF—Arbitrary EtherType in hex
- **aarp**—EtherType: AppleTalk ARP
- **amber**—EtherType: DEC-Amber
- **appletalk**—EtherType: AppleTalk/EtherTalk
- **dec-spanning**—EtherType: DEC-Spanning-Tree
- **decnet-iv**—EtherType: DECnet Phase IV
- **diagnostic**—EtherType: DEC-Diagnostic
- **dsm**—EtherType: DEC-DSM
- **etype-6000**—EtherType: 0x6000
- **etype-8042**—EtherType: 0x8042
- **ip**—EtherType: 0x0800
- **ipx-arpa**—IPX arpa
- **ipx-non-arpa**—IPX non arpa
- **lat**—EtherType: DEC-LAT
- **lavc-sca**—EtherType: DEC-LAVC-SCA
- **mop-console**—EtherType: DEC-MOP Remote Console
- **mop-dump**—EtherType: DEC-MOP Dump
- **msdos**—EtherType: DEC-MSDOS
- **mumps**—EtherType: DEC-MUMPS
- **netbios**—EtherType: DEC-NETBIOS
- **vines-echo**—EtherType: VINES Echo

- **vines-ip**—EtherType: VINES IP
- **xns-idp**—EtherType: XNS IDP

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

- Enter MAC addresses as three 4-byte values in dotted hexadecimal format (for example, 0030.9629.9f84).
- Enter 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*, you can enter either the EtherType or the keyword.
- Entries without a *protocol* match any protocol.
- Access lists 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.

Malformed, invalid, deliberately corrupt EtherType 0x800 IP frames are not recognized as IP traffic and are not filtered by IP ACLs.

An ACE created with the **mac access-list extended** command with the **ip** keyword filters malformed, invalid, deliberately corrupt EtherType 0x800 IP frames only; it does not filter any other IP traffic.

Examples

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

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dsm
Router(config-ext-macl)# permit any any
```

Related Commands

Command	Description
show mac-address-table	Displays information about the MAC-address table.

mac-address-table aging-time

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

mac-address-table aging-time *seconds* [**routed-mac** | **vlan** *vlan-id*]

no mac-address-table aging-time *seconds* [**routed-mac** | **vlan** *vlan-id*]

Syntax Description

seconds	Aging time; valid values are 0 and from 5 to 1000000 seconds.
routed-mac	(Optional) Specifies the routed MAC aging interval.
vlan *vlan-id*	(Optional) Specifies the VLAN to apply the changed aging time; valid values are from 1 to 4094.

Command Default

300 seconds

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

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

Enter **0** seconds to disable aging.

You can enter the **routed-mac** keyword to configure the MAC address aging time for traffic that has the routed MAC (RM) bit set.

Examples

This example shows how to configure the aging time:

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

This example shows how to change the RM aging time:

```
Router(config)# mac-address-table aging-time 500 routed-mac
Router(config)#
```

This example shows how to disable aging:

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

Related Commands

Command	Description
show mac-address-table	Displays information about the MAC-address table.

mac-address-table learning

To enable MAC-address learning, use the **mac-address-table learning** command. To disable learning, use the **no** form of this command.

[**default**] **mac-address-table learning** {{**vlan** *vlan-id*} | {**vlans** *vlan-range*} | {**interface** *interface slot/port*}} [**module** *num*]

no mac-address-table learning {{**vlan** *vlan-id*} | {**vlans** *vlan-range*} | {**interface** *interface slot/port*}} [**module** *num*]

Syntax Description

default	(Optional) Returns to the default settings.
vlan *vlan-id*	Specifies the VLAN to apply the per-VLAN learning of all MAC addresses; valid values are from 1 to 4094.
vlans *vlan-range*	Specifies the number of the VLANs to be mapped to the specified instance; valid values are from 1 to 4094.
interface	Specifies per-interface based learning of all MAC addresses.
interface slot/port	Interface type, the slot number, and the port number.
module *num*	(Optional) Specifies the module number.

Command Default

If you configure a VLAN on a port in a module, all the supervisor engines and DFCs in the Catalyst 6500 series switch are enabled to learn all the MAC addresses on the specified VLAN.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.
12.(23)SXH	This command was changed to allow you to enter a range of VLANs.

Usage Guidelines

You can use the **module** *num* keyword and argument to specify supervisor engines or DFCs only.

You can use the **vlan** *vlan-id* keyword and argument on switch-port VLANs only. You cannot use the **vlan** *vlan-id* keyword and argument to configure learning on routed interfaces.

You can use the **interface** *interface slot/port* keyword and arguments on routed interfaces and supervisor engines only. You cannot use the **interface** *interface slot/port* keyword and arguments to configure learning on switch-port interfaces.

In releases after Cisco IOS Release 12.(23)SXH, you can enter a range of VLANS separated by a hyphen.

Examples

This example shows how to enable MAC-address learning on a switch-port interface on all modules:

```
Router (config)# mac-address-table learning vlan 100
Router (config)#
```

This example shows how to enable MAC-address learning on a range of VLANs on all modules:

```
Router (config)# mac-address-table learning vlan 100-115,125
Router (config)#
```

This example shows how to enable MAC-address learning on a switch-port interface on a specified module:

```
Router (config)# mac-address-table learning vlan 100 module 4
Router (config)#
```

This example shows how to disable MAC-address learning on a specified switch-port interface for all modules:

```
Router (config)# no mac-address-table learning vlan 100
Router (config)#
```

This example shows how to enable MAC-address learning on a routed interface on all modules:

```
Router (config)# mac-address-table learning vlan 100
Router (config)#
```

This example shows how to enable MAC-address learning on a routed interface for a specific module:

```
Router (config)# mac-address-table learning interface FastEthernet 3/48 module 4
Router (config)#
```

This example shows how to disable MAC-address learning for all modules on a specific routed interface:

```
Router (config)# no mac-address-table learning interface FastEthernet 3/48
Router (config)#
```

Related Commands

Command	Description
show mac-address-table learning	Displays the MAC-address learning state.

mac-address-table limit

To enable MAC limiting, use the **mac-address-table limit** command. To disable MAC limiting, use the **no** form of this command.

mac-address-table limit [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**notification** {**syslog** | **trap** | **both**}]

mac-address-table limit [{**vlan** *vlan*} | {**interface** *type mod/port*}] [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

no mac-address-table limit [**vlan** *vlan*] [**maximum** | **action**]

Syntax Description

maximum *num*	(Optional) Specifies the maximum number of MAC entries per VLAN per EARL allowed; valid values are from 5 to 32000 MAC-address entries.
action	(Optional) Specifies the type of action to be taken when the action is violated.
warning	Specifies that the one syslog message will be sent and no further action will be taken when the action is violated.
limit	Specifies that the one syslog message will be sent and/or a corresponding trap will be generated with the MAC limit when the action is violated.
shutdown	Specifies that the one syslog message will be sent and/or the VLAN is moved to the blocked state when the action is violated.
notification	(Optional) Specifies the type of notification to be sent when the action is violated.
syslog	Sends a syslog message when the action is violated.
trap	Sends trap notifications when the action is violated.
both	Sends syslog and trap notifications when the action is violated.
vlan *vlan*	(Optional) Enables MAC limiting on a per-VLAN basis.
interface *type mod/port*	(Optional) Enables MAC limiting on a per-port basis.
flood	(Optional) Enables unknown unicast flooding on a VLAN.

Command Default

The defaults are as follows:

- **maximum** *num* is **500** MAC address entries.
- **action** is **warning**.
- **notification** is **syslog**.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use this syntax for enabling MAC limiting globally:

mac-address-table limit [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**notification** {**syslog** | **trap** | **both**}]

Use this syntax for enabling per-VLAN MAC limiting:

mac-address-table limit [**vlan** *vlan*] [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

Use this syntax for enabling per-port MAC limiting:

mac-address-table limit [**interface** *type mod/port*] [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

If you enable per-VLAN MAC limiting, the per-VLAN MAC limiting supersedes the **mac-address-table limit** command that globally enables MAC limiting.

The maximum number of MAC entries is based per VLAN and per EARL.

If you do not specify a maximum, an action, or a notification, the default settings are used.

If you enable per-VLAN MAC limiting, MAC limiting is enabled on the VLAN specified only.

The **flood** keyword is supported on VLAN interfaces only.

The **flood** action occurs only if the **limit** action is configured and is violated.

In the **shutdown** state, the VLAN remains in the blocked state until you reenable it through the CLI.

Examples

This example shows how to enable the MAC limit globally:

```
Router(config)# mac-address-table limit
Router(config)#
```

This example shows how to enable per-VLAN MAC limiting:

```
Router(config)# mac-address-table limit vlan 501 maximum 50 action shutdown
Router(config)#
```

Related Commands

Command	Description
show mac-address-table limit	Displays the information about the MAC-address table.

mac-address-table notification mac-move

To enable MAC-move notification, use the **mac-address-table notification mac-move** command. To disable MAC-move notification, use the **no** form of this command.

mac-address-table notification mac-move

no mac-address-table notification mac-move

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

MAC-move notification generates a syslog message whenever a MAC address or host moves between different switch ports.

MAC-move notification does not generate a notification when a new MAC address is added to the CAM or when a MAC address is removed from the CAM.

MAC-move notification is supported on switch ports only.

Examples

This example shows how to enable MAC-move notification:

```
Router(config)# mac-address-table notification mac-move
Router(config)#
```

This example shows how to disable MAC-move notification:

```
Router(config)# no mac-address-table notification mac-move
Router(config)#
```

Related Commands

Command	Description
show mac-address-table notification mac-move	Displays the information about the MAC-address table.

mac-address-table notification threshold

To enable CAM table usage monitoring notification, use the **mac-address-table notification threshold** command. To disable CAM table usage monitoring notification, use the **no** form of this command.

mac-address-table notification threshold {**limit** *percentage*} {**interval** *time*}

no mac-address-table notification threshold

Syntax Description

limit *percentage*	Specifies the percentage of the CAM utilization; valid values are from 1 to 100 percent.
interval *time*	Specifies the time between notifications; valid values are greater than or equal to 120 seconds.

Command Default

The defaults are as follows:

- Disabled.
- *percentage* is **50** percent.
- *time* is **120** seconds.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When you enable CAM table usage monitoring, the number of valid entries in the CAM table are counted and if the percentage of the CAM utilization is higher or equal to the specified threshold, a message is displayed.

Examples

This example shows how to enable CAM table usage monitoring notification and use the default settings:

```
Router(config)# mac-address-table notification threshold
Router(config)#
```

This example shows how to enable CAM table usage monitoring notification and set the threshold and interval:

```
Router(config)# mac-address-table notification threshold limit 20 interval 200
Router(config)#
```

This example shows how to disable CAM table usage monitoring notification:

```
Router(config)# no mac-address-table notification threshold
Router(config)#
```

Related Commands

Command	Description
show mac-address-table notification threshold	Displays information about the MAC-address table.

mac-address-table static

To add static entries to the MAC-address table or configure a static MAC address with IGMP snooping disabled for that address, use the **mac-address-table static** command. See the "Usage Guidelines" section for information about the **no** form of this command.

mac-address-table static *mac-addr* **vlan** *vlan-id* {**interface** *type* | **drop** [**disable-snooping**]} [**dlci** *dlci* | **pvc** *vpi/vci*] [**auto-learn** | **disable-snooping**] [**protocol** {**ip** | **ipv6** | **ipx** | **assigned**}]

no mac-address-table static *mac-addr* {**vlan** *vlan-id*} {**interface** *type*} [**disable-snooping**] [**dlci** *dlci* | **pvc** *vpi/vci*]

Syntax Description

mac-addr	Address to add to the MAC-address table.
vlan *vlan-id*	Specifies the VLAN to apply the changed aging time; valid values are from 1 to 4094.
interface *type*	Specifies the interface type and module/port number.
drop	Drops all traffic that is received from and going to the configured MAC address in the specified VLAN.
disable-snooping	(Optional) Disables IGMP snooping on the multicast MAC address.
dlci *dlci*	(Optional) Specifies mapping the DLCI to this MAC address; valid values are from 16 to 1007.
pvc *vpi/vci*	(Optional) Specifies mapping the PVC to this MAC address.
auto-learn	(Optional) Updates the entry with the new port; see the "Usage Guidelines" section for additional information.
protocol	(Optional) Specifies the protocol that is associated with the entry.
ip	Specifies the IP protocol.
ipv6	Specifies the IPv6 protocol.
ipx	Specifies the IPX protocol.
assigned	Specifies assigned protocol bucket accounts for such protocols as DECnet, Banyan VINES, and AppleTalk.

Command Default

This command has no default settings.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Use the **no** form of this command to do the following:

- Remove entries that are profiled by the combination of specified entry information.

- Note that IGMP snooping is not disabled for the specified address.
- Remove the MAC address to a Frame Relay DLCI or ATM PVC mapping.

The **dlci** *dlci* keyword and argument are valid only if Frame Relay encapsulation has been enabled on the specified interface.

The **pvc** *vpi/vci* keyword and arguments are supported on ATM interfaces only.

When specifying the **pvc** *vpi/vci*, you must specify both a VPI and a VCI, separated by a slash.

When you install a static MAC address, it is associated with a port. If the same MAC address is seen on a different port, the entry is updated with the new port if you enter the **auto-learn** keyword.

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

The **ipx** keyword is not supported.

You can enter up to 15 interfaces per command entered, but you can enter more interfaces by repeating the command.

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 system MAC addresses.

When removing a MAC address, entering **interface** *type* 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.

The **mac-address-table static** *mac-addr* {**vlan** *vlan-id*} {**interface** *type*} **disable-snooping** command disables snooping on the specified static MAC entry/VLAN pair only. To reenable snooping, you must first delete the MAC address and then reinstall it using the **mac-address-table static** *mac-addr* {**vlan** *vlan-id*} {**interface** *type*} command without entering the **disable-snooping** keyword.

The **mac-address-table static** *mac-addr* {**vlan** *vlan-id*} **drop** command cannot be applied to a multicast MAC address.

To support multipoint bridging and other features, you must also specify the **dlci** *dlci* keyword and argument for Frame Relay interfaces or the **pvc** *vpi/vci* keyword and arguments for ATM interfaces as follows:

```
Router(config)# mac-address-table static 000C.0203.0405 vlan 101 interface ATM6/1 pvc6/101
Router(config)#
```

Note If you omit the **dlci** *dlci* keyword and argument for Frame Relay interfaces, the MAC address is mapped to the first DLCI circuit that is configured for the specified VLAN on that interface. If you omit the **pvc** *vpi/vci* keyword and arguments for ATM interfaces, the MAC address is mapped to the first PVC circuit that is configured for the specified VLAN on that interface. To ensure that the MAC address is configured correctly, we recommend that you always use the **dlci** *dlci* and **pvc** *vpi/vci* keywords and arguments on the appropriate interfaces.

Examples

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

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

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

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

This example shows how to add static entries to the MAC address table for an ATM PVC circuit and for a Frame Relay DLCI circuit:

```
Router(config)# mac-address-table static 0C01.0203.0405 vlan 101 interface ATM6/1 pvc 6/101
Router(config)# mac-address-table static 0C01.0203.0406 vlan 202 interface POS4/2 dlci 200
Router(config)#
```

Related Commands

Command	Description
show mac-address-table	Displays information about the MAC-address table.

mac-address-table synchronize

To synchronize the Layer 2 MAC address table entries across the PFC and all the DFCs, use the **mac-address-table synchronize** command. To disable MAC address table synchronization or reset the activity timer, use the **no** form of this command.

mac-address-table synchronize [**activity-time** *seconds*]

no mac-address-table synchronize [**activity-time** *seconds*]

Syntax Description

activity-time *seconds*	(Optional) Specifies the activity timer interval: valid values are **160**, **320**, and **640** seconds.

Command Default

The default settings are as follows:

- Disabled.
- Enabled for WS-X6708-10GE.
- **activity-time** is 160 seconds.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

We recommend that you configure the activity time so that at least two activity times exist within the regular Layer 2 aging time (or within the aging time used for VLANs in distributed EtherChannels if this feature is used only for distributed EtherChannels). If at least two activity times do not exist within the aging time, then an error message is displayed.

Examples

This example shows how to specify the activity timer interval:

```
Router(config)# mac-address-table synchronize activity-time 320
Router(config)#
```

Related Commands

Command	Description
show mac-address-table synchronize statistics	Displays information about the MAC-address table.

mac packet-classify

To classify Layer 3 packets as Layer 2 packets, use the **mac packet-classify** command. To return to the default settings, use the **no** form of this command.

mac packet-classify

no mac packet-classify

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

PFC3BXL and PFC3B modes support protocol-independent MAC ACL filtering. Protocol-independent MAC ACL filtering applies MAC ACLs to all ingress traffic types (for example, IPv4 traffic, IPv6 traffic, and MPLS traffic, in addition to MAC-layer traffic).

You can configure these interface types for multilayer MAC ACL QoS filtering:

- VLAN interfaces without Layer 3 addresses
- Physical LAN ports that are configured to support EoMPLS
- Logical LAN subinterfaces that are configured to support EoMPLS

The ingress traffic that is permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering is processed by egress interfaces as MAC-layer traffic. You cannot apply egress IP ACLs to traffic that was permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering.

Microflow policing does not work on interfaces that have the **mac packet-classify** command enabled.

The **mac packet-classify** command causes the Layer 3 packets to be classified as Layer 2 packets and disables IP classification.

Traffic is classified based on 802.1Q CoS, trunk VLAN, EtherType, and MAC addresses.

Examples

This example shows how to classify incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

This example shows how to disable the classification of incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

Related Commands

Command	Description
mac packet-classify use vlan	Enables VLAN-based QoS filtering in the MAC ACLs.

mac packet-classify use vlan

To enable VLAN-based QoS filtering in the MAC ACLs, use the **mac packet-classify use vlan** command. To return to the default settings, use the **no** form of this command.

mac packet-classify use vlan

no mac packet-classify use vlan

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

PFC3BXL and PFC3B modes support protocol-independent MAC ACL filtering. Protocol-independent MAC ACL filtering applies MAC ACLs to all ingress traffic types (for example, IPv4 traffic, IPv6 traffic, and MPLS traffic, in addition to MAC-layer traffic).

You must use the **no mac packet-classify use vlan** command to disable the VLAN field in the Layer 2 key if you want to apply QoS to the Layer 2 SAP-encoded packets (for example, IS-IS and IPX).

QoS does not allow policing of non-ARPA Layer 2 packets (for example, IS-IS and IPX) if the VLAN field is enabled.

Examples

This example shows how to enable VLAN-based QoS filtering in the MAC ACLs:

```
Router(config)# mac packet-classify use vlan
Router(config)
```

This example shows how to disable VLAN-based QoS filtering in the MAC ACLs:

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

Related Commands

Command	Description
mac packet-classify	Classifies Layer 3 packets as Layer 2 packets.

match

To specify the match clause by selecting one or more ACLs for a VLAN access-map sequence, use the **match** subcommand. The match clause specifies the IP, IPX, or MAC ACLs for traffic filtering. To remove the match clause, use the **no** form of this command.

match {**ip address** {*acl-number* | *acl-name*}} | {**ipx address** {*acl-number* | *acl-name*} | {**mac address** *acl-name*}}

no match {**ip address** {*acl-number* | *acl-name*}} | {**ipx address** {*acl-number* | *acl-name*} | {**mac address** *acl-name*}}

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.
ipx address *acl-number*	Selects one or more IPX ACLs for a VLAN access-map sequence; valid values are from 800 to 999.
ipx address *acl-name*	Selects an IPX ACL by name.
mac address *acl-name*	Selects one or more MAC ACLs for a VLAN access-map sequence.

Command Default

This command has no default settings.

Command Modes

VLAN access-map submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **match ipx address** and **match mac address** commands are not supported for VACLs on WAN interfaces.

IPX ACLs that are used in VACLs can only specify the IPX protocol type, the source network, the destination network, and the destination host address.

The MAC sequence is not effective for IP or IPX packets. IP packets and IPX packets should be access controlled by IP and IPX match clauses.

You cannot configure VACLs on secondary VLANs. The secondary VLAN inherits all features that are configured on the primary VLAN.

These subcommands appear in the CLI help but are not supported by the PFC QoS:

- **match cos**
- **match any**
- **match class-map**
- **match destination-address**

- **match input-interface**
- **match qos-group**
- **match source-address**

Refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional configuration guidelines and restrictions.

Refer to the *Cisco IOS Release 12.2 Command Reference* publication for additional **match** command information.

Examples

This example shows how to define a match clause for a VLAN access map:

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address 13
Router(config-access-map)#
```

Related Commands

Command	Description
action	Sets the packet action clause.
port access-map	Creates a port access map or enters port access-map command mode.
show vlan access-map	Displays the contents of a VLAN-access map.
vlan access-map	Creates a VLAN access map or enters VLAN access-map command mode.

match protocol

To configure the match criteria for a class map on the basis of the specified protocol, use the **match protocol** command. To remove the protocol-based match criteria from a class map, use the **no** form of this command.

match protocol {**ip** | **ipv6**}

no match protocol {**ip** | **ipv6**}

Syntax Description

ip	Specifies protocol matching on IP packets.
ipv6	Specifies protocol matching on IPv6 packets.

Command Default

This command has no default settings.

Command Modes

Class-map submode

Command History

12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **match protocol** class-map subcommand configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in the software on the PISA.

For class-based weighted fair queueing, you define traffic classes based on match criteria including protocols, ACLs, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class to which you want to establish the match criteria.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

This command can be used to match protocols that are known to the NBAR feature. For a list of protocols currently supported by NBAR, see the "Classification" section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

This example shows how to specify a class map called ip and configure the IP as a match criterion for it:

```
Router(config)# class-map ip
Router(config-cmap)# match protocol ip
```

maxconns (real server configuration submode)

To limit the number of active connections to the real server, use the **maxconns** command. To change the maximum number of connections to the default settings, use the **no** form of this command.

maxconns *number-conns*

no maxconns

Syntax Description

number-conns	Maximum number of active connections on the real server at any one point in time; valid values are from 0 to 4294967295.

Command Default

0

Command Modes

Real server configuration submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you do not specify the *number-conns* value, the default value is **0**, which means that the maximum number of connections to the real server are not monitored.

Examples

This example shows how to limit the number of active connections to the real server:

```
Router(config-if)# maxconns 49672
Router(config-if)#
```

This example shows how to revert to the default settings:

```
Router(config-if)# no maxconns
Router(config-if)#
```

Related Commands

Command	Description
faildetect numconns	Specifies the conditions that indicate a server failure.
inservice (real server)	Enables the real server for use by the Cisco IOS SLB feature.
reassign	Defines the number of consecutive number of SYNs for a new connection that will go unanswered before the connection is attempted to a different real server.
retry	Defines the amount of time that must elapse before a connection is attempted to a failed server.

maximum-paths

To control the maximum number of parallel routes that an IP routing protocol can support, use the **maximum-paths** command. To restore the default settings, use the **no** form of this command.

maximum-paths *maximum*

no maximum-paths

Syntax Description

maximum	Maximum number of parallel routes that an IP routing protocol installs in a routing table; valid values are from 1 to 8.

Command Default

The defaults are as follows:

- BGP has one path.
- All other IP routing protocols have four paths.

Command Modes

Routing protocol configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to allow a maximum of two paths to a destination:

```
Router(config-router)# maximum-paths 2
Router(config-router)
```

mdix auto

To enable automatic media-dependent interface with crossover detection, use the **mdix auto** command. To turn automatic detection off, use the **no** form of this command.

mdix auto

no mdix auto

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is supported on the following modules only:

- WS-X6748-GE-TX
- WS-SUP720 (copper ports only)
- WS-SUP720-10G (copper ports only)
- WS-SUP32 (copper ports only)
- WS-X6148A-RJ45
- WS-X6148A-GE-TX
- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6548-GE-TX
- WS-X6516-GE-TX
- WS-X6148-GE-TX
- WS-X6148X2-RJ45
- WS-X6196-RJ21
- The copper SFP (GLC-T) and the copper GBIC (WS-G5483) also support automatic MDIX when used in one of the modules that support these tranceivers.

Examples

This example shows how to enable automatic media-dependent interface with crossover detection:

```
Router# mdix auto
Router#
```

This example shows how to disable automatic media-dependent interface with crossover detection:

```
Router# no mdix auto
Router#
```

mdt data

To configure the multicast group address range for data MDT groups, use the **mdt data** command. To disable this function, use the **no** form of this command.

mdt data *group-address-range wildcard-bits* [**threshold** *threshold-value*] [**list** *access-list*]

no mdt data *group-address-range wildcard-bits* [**threshold** *threshold-value*] [**list** *access-list*]

Syntax Description

group-address-range	Multicast group address range; valid values are from 224.0.0.1 to 239.255.255.255.
wildcard-bits	Wildcard bits to be applied to the multicast group address range.
threshold *threshold-value*	(Optional) Defines the bandwidth threshold value; valid values are from 1 through 4294967.
list *access-list*	(Optional) Defines the access-list name or number.

Command Default

Disabled

Command Modes

VRF configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

A data MDT group can include a maximum of 256 multicast groups per VPN. Multicast groups that are used to create the data MDT group are dynamically chosen from a pool of configured IP addresses.

This command configures a range of alternative multicast destination addresses for the tunnel header. The destination address chosen depends on the traffic profile (the source and destination match the specified access list and the rate of the traffic has exceeded the bandwidth threshold value).

Examples

This example shows how to configure the multicast group address range for data MDT groups:

```
Router(config-vrf)# mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
Router(config-vrf)#
```

Related Commands

Command	Description
mdt default	Configures a default MDT group for a VRF instance.

mdt default

To configure a default MDT group for a VRF instance, use the **mdt default** command in VRF configuration mode. To disable this function, use the **no** form of this command.

mdt default *group-address*

no mdt default *group-address*

Syntax Description

group-address	IP address of the default MDT group.

Command Default

Disabled

Command Modes

VRF configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The default MDT group must be the same group that is configured on all provider-edge routers that belong to the same VPN.

The *group-address* serves as an identifier for the community because provider-edge routers that are configured with the same group address become members of the group, allowing them to receive packets that are sent by each other.

If you use the SSM protocol for the default MDT, the source IP address is used to source the BGP sessions.

A tunnel interface is created when you enter this command. By default, the destination address of the tunnel header is the *group-address* argument.

Examples

This example shows how to configure a default MDT group for a VRF instance:

```
Router(config-vrf)# mdt default 232.0.0.1
Router(config-vrf)#
```

Related Commands

Command	Description
mdt data	Configures the multicast group address range for data MDT groups.

mdt log-reuse

To enable the recording of data MDT reuse, use the **mdt log-reuse** command in VRF configuration mode. To disable this function, use the **no** form of this command.

mdt log-reuse

no mdt log-reuse

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

VRF configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **mdt log-reuse** command generates a syslog message whenever a data MDT is reused.

Examples

This example shows how to enable the MDT log reuse function:

```
Router(config-vrf)# mdt log-reuse
Router(config-vrf)#
```

Related Commands

Command	Description
mdt data	Configures the multicast group address range for data MDT groups.
mdt default	Configures a default MDT group for a VRF instance.

media-type

To select the connector to use for the dual-mode uplink port, use the **media-type** command. To return to the default settings, use the **no** form of this command.

media-type {**rj45** | **sfp**}

no media-type

Syntax Description

rj45	Uses an RJ-45 connector.
sfp	Uses an SFP connector.

Command Default

sfp

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Port 1 has a small form-factor pluggable (SFP) connector.

Port 2 has an RJ-45 connector and an SFP connector. You must configure the port to use one connector or the other.

Examples

This example shows how to configure port 2 in slot 5 to use the RJ-45 connector:

```
Router(config)# interface gigabitethernet 5/2
Router(config-if)# media-type rj45
```

mkdir disk0:

To create a new directory in a flash file system, use the **mkdir disk0:** command.

mkdir disk0:

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command is valid only on flash file systems.

After you enter the **mkdir disk0:** command, you are prompted to enter the new directory filename.

To check your entry, enter the **dir** command.

To remove a directory, enter the **rmdir** command.

Examples

This example shows how to create a directory named newdir:

```
Router# mkdir disk0:
Create directory filename [ ]? newdir
Created dir disk0: newdir
Router#
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
rmdir	Removes an existing directory in a Class C flash file system.

mls aclmerge algorithm

To select the type of ACL merge method to use, use the **mls aclmerge algorithm** command.

mls aclmerge algorithm {**bdd** | **odm**}

Syntax Description

bdd	Specifies the BDD-based algorithm.
odm	Specifies the ODM-based algorithm.

Command Default

bdd

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The BDD-based ACL merge uses Boolean functions to condense entries into a single merged list of TCAM entries that can be programmed into the TCAM.

You cannot disable the ODM-based ACL merge on Catalyst 6500 series switches.

The ODM-based ACL merge uses an order-dependent merge algorithm to process entries that can be programmed into the TCAM.

Note The ODM-based ACL merge supports both security ACLs and ACLs that are used for QoS filtering.

If you change the algorithm method, the change is not retroactive. For example, ACLs that have had the merge applied are not affected. The merge change applies to future merges only.

Use the **show fm summary** command to see the status of the current merge method.

Examples

This example shows how to select the BDD-based ACL to process ACLs:

```
Router(config)# mls aclmerge algorithm bdd
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)
```

This example shows how to select the ODM-based ACL merge to process ACLs:

```
Router(config)# mls aclmerge algorithm odm
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)#
```

Related Commands

Command	Description
show fm summary	Displays a summary of feature manager information.

mls acl tcam default-result

To set the default action during the ACL TCAM update, use the **mls acl tcam default-result** command. To return to the default settings, use the **no** form of this command.

mls acl tcam default-result {**permit** | **deny** | **bridge**}

no mls acl tcam default-result

Syntax Description

permit	Permits all traffic.
deny	Denies all traffic.
bridge	Bridges all Layer 3 traffic up to MSFC, RP, or the software.

Command Default

deny

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

In the transition time between when an existing ACL is removed and a new ACL is applied, a default **deny** is programmed in the hardware. Once the new ACL has been applied completely in the hardware, the default **deny** is removed.

Use the **mls acl tcam default-result permit** command to permit all traffic in the hardware or bridge all traffic to the software during the transition time.

Examples

This example shows how to permit all traffic to pass during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result permit
Router(config)#
```

This example shows how to deny all traffic during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result deny
Router(config)#
```

This example shows how to bridge all Layer 3 traffic during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result bridge
Router(config)#
```

mls acl tcam share-global

To enable sharing of the global default ACLs, use the **mls acl tcam share-global** command. To turn off sharing of the global defaults, use the **no** form of this command.

mls acl tcam share-global

no mls acl tcam share-global

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to enable sharing of the global default ACLs:

```
Router(config)# mls acl tcam share-global
Router(config)#
```

mls aging fast

To configure the fast-aging time for unicast entries in the Layer 3 table, use the **mls aging fast** command. To restore the MLS fast-aging time to the default settings, use the **no** form of this command.

mls aging fast [{**threshold** *packet-count*} [{**time** *seconds*}]]

mls aging fast [{**time** *seconds*} [{**threshold** *packet-count*}]]

no mls aging fast

Syntax Description

threshold *packet-count*	(Optional) Specifies the packet count of the fast-aging threshold for Layer 3 fast aging; valid values are from 1 to 128.
time *seconds*	(Optional) Specifies how often entries are checked; valid values are from 1 to 128 seconds.

Command Default

The defaults are as follows:

- Fast aging is disabled.
- If fast aging is enabled, the default *packet-count* value is 100 packets and the *seconds* default is 32 seconds.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.

Examples

This example shows how to configure the MLS fast-aging threshold:

```
Router(config)# mls aging fast threshold 50
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls aging long

To configure the long-aging time for unicast entries in the Layer 3 table, use the **mls aging long** command. To restore the MLS long-aging time to the default settings, use the **no** form of this command.

mls aging long *seconds*

no mls aging long

Syntax Description

seconds	Layer 3 long-aging timeout; valid values are from 64 to 1920 seconds.

Command Default

1920 seconds

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.

Examples

This example shows how to configure the MLS long-aging threshold:

```
Router(config)# mls aging long 800
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls aging normal

To configure the normal-aging time for unicast entries in the Layer 3 table, use the **mls aging normal** command. To restore the MLS normal-aging time to the default settings, use the **no** form of this command.

mls aging normal *seconds*

no mls aging normal

Syntax Description

seconds	Normal aging timeout for Layer 3; valid values are from 32 to 4092 seconds.

Command Default

300 seconds

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.

Examples

This example shows how to configure the MLS normal-aging threshold:

```
Router(config)# mls aging normal 200
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls cef maximum-routes

To limit the maximum number of the routes that can be programmed in the hardware allowed per protocol, use the **mls cef maximum-routes** command. To return to the default settings, use the **no** form of this command.

mls cef maximum-routes {**ip** *maximum-routes*} | {**ip-multicast** *maximum-routes*} |
{**ipv6** *maximum-routes*} | {**mpls** *maximum-routes*}

no mls cef maximum-routes {**ip** | **ip-multicast** | **ipv6** | **mpls**}

Syntax Description

ip	Specifies the maximum number of IP routes.
maximum-routes	Maximum number of the routes that can be programmed in the hardware allowed per protocol; see the "Usage Guidelines" section for valid values.
ip-multicast	Specifies the maximum number of multicast routes.
ipv6	Specifies the maximum number of IPv6 routes.
mpls	Specifies the maximum number of MPLS labels.

Command Default

The defaults are as follows:

- For XL-mode systems:
  - IPv4 unicast and MPLS—512,000 routes
  - IPv6 multicast/unicast and IPv4 multicast—256,000 routes
- For non-XL mode systems:
  - IPv4 unicast and MPLS—192,000 routes
  - IPv6 multicast/unicast and IPv4 multicast—32,000 routes

Note The size of the global Internet routing table plus any local routes might exceed the non-XL mode default partition sizes. See the "Usage Guidelines" section for additional information.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Note If you copy a configuration file that contains the MLS CEF maximum routes into the startup-config file and reload the Catalyst 6500 series switch, the Catalyst 6500 series switch reloads after it reboots.

The **mls cef maximum-routes** command limits the maximum number of the routes that can be programmed in the hardware. If routes are detected that exceed the limit for that protocol, an exception condition is generated.

The XL and non-XL modes are based on the type of PFC module that is installed in your system. You cannot configure the mode except by the installed hardware. The Supervisor Engine 32 PISA contains a PFC3B and is considered a non-XL mode system.

The valid values for *max-routes* are as follows:

- IP and MPLS— Up to 239,000 routes
- IP-multicast and IPv6 multicast/unicast—Up to 119,000 routes

Note The maximum values that you are permitted to configure is not fixed but varies depending on the values that are allocated for other protocols.

An example of how to enter the maximum routes argument is as follows:

```
Router(config)# mls cef maximum-routes ip 4
```

where 4 is 4096 IP routes (1024 x4 = 4096).

The new configurations are applied after a system reload only and do not take effect if a switchover occurs.

In RPR mode, if you change and save the maximum-routes configuration, the redundant supervisor engine reloads when it becomes active from either a switchover or a system reload. The reload occurs 5 minutes after the supervisor engine becomes active.

Use the **show mls cef maximum-routes** command to view the current maximum routes system configuration.

Examples

This example shows how to set the maximum number of routes that are allowed per protocol:

```
Router(config)# mls cef maximum-routes ip 100
Router(config)#
```

This example shows how to return to the default setting for a specific protocol:

```
Router(config)# no mls cef maximum-routes ip
Router(config)#
```

Related Commands

Command	Description
show mls cef maximum-routes	Displays the current maximum-route system configuration.

mls cef tunnel fragment

To allow tunnel fragmentation, use the **mls cef tunnel fragment** command. To return to the default settings, use the **no** form of this command.

mls cef tunnel fragment

no mls cef tunnel fragment

Command Default

Disabled

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When you enable tunnel fragmentation, if the size of the packets that are going into a tunnel interface exceed the MTU, the packet is fragmented. The packets that are fragmented are reassembled at the destination point.

Examples

This example shows how to allow tunnel fragmentation:

```
Router(config)# mls cef tunnel fragment
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls cef tunnel fragment
Router(config)#
```

Related Commands

Command	Description
show mls cef tunnel fragment	Displays the operational status of tunnel fragmentation.

mls erm priority

To assign the priorities to define an order in which protocols attempt to recover from the exception status, use the **mls erm priority** command. To return to the default settings, use the **no** form of this command.

mls erm priority {**ipv4** *value*} {**ipv6** *value*} {**mpls** *value*}

no mls erm priority {**ipv4**} {**ipv6**} {**mpls**}

Syntax Description

ipv4	Prioritizes the IPv4 protocol.
value	Priority value; valid values are from 1 to 3.
ipv6	Prioritizes the IPv6 protocol.
mpls	Prioritizes the MPLS protocol.

Command Default

The default settings are as follows:

- **ipv4** is **1**.
- **ipv6** is **2**.
- **mpls** is **3**.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

A lower *value* indicates a higher priority.

When a protocol sees a FIB table exception, the protocol notifies the FIB ERM manager. The FIB ERM manager periodically polls the FIB table exception status and decides which protocol gets priority over another protocol when multiple protocols are running under the exception. Only one protocol can attempt to recover from an exception at any time.

If there is sufficient FIB space, the protocol with the highest priority tries to recover first. Other protocols under the exception do not start to recover until the previous protocol completes the recovery process by reloading the appropriate FIB table.

Examples

This example shows how to set the ERM exception-recovery priority:

```
Router(config)# mls erm priority ipv4 1 ipv6 2 mpls 3
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls erm priority ipv4 ipv6 mpls
Router(config)#
```

Related Commands

Command	Description
show mls cef exception	Displays information about the CEF exception.

mls exclude protocol

To specify the interface protocol to exclude from shortcutting, use the **mls exclude protocol** command. To remove a prior entry, use the **no** form of this command.

mls exclude protocol {{**both** | **tcp** | **udp**}{**port** *port-number*}}

no mls exclude

Syntax Description

both	Specifies both UDP and TCP.
tcp	Excludes TCP interfaces from shortcutting.
udp	Specifies UDP interfaces from shortcutting.
port *port-number*	Specifies the port number; valid values are from 1 to 65535.

Command Default

This command has no default settings.

Command Modes

Global configuration (config) (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Examples

This example shows how to configure MLS to exclude UDP on port 69:

```
Router(config)# mls exclude protocol udp port 69
Router(config)#
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.