mls flow

To configure the flow mask for NDE, use the **mls flow** command. To restore the flow mask to the default, use the **no** form of this command.

mls flow {{**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**}}

no mls flow {**ip** | **ipv6**}

Syntax Description

ip	Enables the flow mask for MLS IP packets.
ipv6	Enables the flow mask for MLS IPv6 packets.
destination	Uses the destination IP address as the key to the Layer 3 table.
destination-source	Uses the destination and the source IP address as the key to the Layer 3 table.
full	Uses the source and destination IP address, the IP protocol (UDP or TCP), and the source and destination port numbers as the keys to the Layer 3 table.
interface-destination-source	Uses all the information in the destination and source flow mask and the source VLAN number as the keys to the Layer 3 table.
interface-full	Uses all the information in the full flow mask and the source VLAN number as the keys to the Layer 3 table.
source	Uses all the information in the source flow mask only.

Command Default

The NDE flow mask is null.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command collects statistics for the supervisor engine.

Examples

This example shows how to set the minimum flow mask for an extended access list for MLS IP:

```
Router(config)# mls flow ip full
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls ip

To enable MLS IP for the internal router on the interface, use the **mls ip** command. To disable MLS IP on the interface, use the **no** form of this command.

mls ip

no mls ip

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast is disabled.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to enable shortcuts for MLS IP:

```
Router(config-if)# mls ip
Router(config-if)#
```

Related Commands

Command	Description
mls rp ip (interface configuration mode)	Allows the external systems to enable MLS IP on a specified interface.
show mls ip multicast	Displays the MLS IP information.

mls ip acl port expand

To enable ACL-specific features for Layer 4, use the **mls ip acl port expand** command. To disable the ACL-specific Layer 4 features, use the **no** form of this command.

mls ip acl port expand

no mls ip acl port expand

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to enable the expansion of ACL logical operations on Layer 4 ports:

```
Router(config)# mls ip acl port expand
Router(config)#
```

mls ip cef accounting per-prefix

To enable MLS per-prefix accounting, use the **mls ip cef accounting per-prefix** command. To disable MLS per-prefix accounting, use the **no** form of this command

mls ip cef accounting per-prefix *prefix-entry prefix-entry-mask* [*instance-name*]

no mls ip cef accounting per-prefix

Syntax Description

prefix	Prefix entry in the format A.B.C.D.
prefix-entry-mask	Prefix entry mask in the format A.B.C.D.
instance-name	(Optional) VPN routing and forwarding instance name.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Per-prefix accounting collects the adjacency counters used by the prefix. When the prefix is used for accounting, the adjacency cannot be shared with other prefixes. You can use per-prefix accounting to account for the packets sent to a specific destination.

Examples

This example shows how to enable MLS per-prefix accounting:

```
Router(config)# mls ip cef accounting per-prefix 172.20.52.18 255.255.255.255
Router(config)#
```

This example shows how to disable MLS per-prefix accounting:

```
Router(config)# no mls ip cef accounting per-prefix
Router(config)#
```

Related Commands

Command	Description
show mls cef ip accounting per-prefix	Displays all the prefixes that are configured for the statistic collection.

mls ip cef load-sharing

To configure the CEF load balancing, use the **mls ip cef load-sharing** command. To return to the default settings, use the **no** form of this command.

mls ip cef load-sharing [**full** [**exclude-port** {**destination** | **source**}]] [**simple**]

no mls ip cef load-sharing

Syntax Description

full	(Optional) Sets the CEF load balancing to include source and destination Layer 4 ports and source and destination IP addresses (Layer 3).
exclude-port destination	(Optional) Excludes the destination Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm.
exclude-port source	(Optional) Excludes the source Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm.
simple	(Optional) Sets the CEF load balancing for single-stage load sharing.

Command Default

Source and destination IP address and universal identification

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **mls ip cef load-sharing** command affects the IPv4, the IPv6, and the MPLS forwardings.

The **mls ip cef load-sharing** command is structured as follows:

- **mls ip cef load-sharing full**—Uses Layer 3 and Layer 4 information with multiple adjacencies.
- **mls ip cef load-sharing full simple**—Uses Layer 3 and Layer 4 information without multiple adjacencies.
- **mls ip cef load-sharing simple**—Uses Layer 3 information without multiple adjacencies.

For additional guidelines, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Examples

This example shows how to set load balancing to include Layer 3 and Layer 4 ports with multiple adjacencies:

```
Router(config)# mls ip cef load-sharing full
Router(config)#
```

This example shows how to set load balancing to exclude the destination Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm:

```
Router(config)# mls ip cef load-sharing full exclude-port destination
Router(config)#
```

This example shows how to set load balancing to exclude the source Layer 4 ports and source and destination IP addresses (Layer 3) from the load-balancing algorithm:

```
Router(config)# mls ip cef load-sharing full exclude-port source
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls ip cef load-sharing
Router(config)#
```

Related Commands

Command	Description
show mls cef ip	Displays the IP entries in the MLS-hardware Layer 3-switching table.

mls ip cef rate-limit

To rate-limit CEF-punted data packets, use the **mls ip cef rate-limit** command. To disable the rate-limited CEF-punted data packets, use the **no** form of this command.

mls ip cef rate-limit *pps*

no mls ip cef rate-limit

Syntax Description

pps	Number of data packets; valid values are from 0 to 1000000.

Command Default

No rate limit is configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Certain denial-of-service attacks target the route processing engines of routers. Certain packets that cannot be forwarded by the PFC are directed to the PISA for processing. Denial-of-service attacks can overload the route processing engine and cause routing instability when running dynamic routing protocols. You can use the **mls ip cef rate-limit** command to limit the amount of traffic that is sent to the PISA to prevent denial-of-service attacks against the route processing engine.

This command rate limits all CEF-punted data packets including the following:

- Data packets going to the local interface IP address
- Data packets requiring ARP

Setting the rate to a low value could impact the packets that are destined to the IP addresses of the local interfaces and the packets that require ARP. You should use this command to limit these packets to a normal rate and to avoid abnormal incoming rates.

For additional guidelines, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Examples

This example shows how to enable and set rate limiting:

```
Router(config)# mls ip cef rate-limit 50000
Router(config)#
```

Related Commands

Command	Description
show mls cef ip	Displays the IP entries in the MLS-hardware Layer 3-switching table.

mls ip cef rpf hw-enable-rpf-acl

To enable hardware uRPF for packets matching the deny ace when uRPF with ACL is enabled, use the **mls ip cef rpf hw-enable-rpf-acl** command. To disable hardware uRPF when RPF and ACL are enabled, use the **no** form of this command.

mls ip cef rpf hw-enable-rpf-acl

no mls ip cef rpf hw-enable-rpf-acl

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you do not enter the **mls ip cef rpf hw-enable-rpf-acl** command, when the uRPF with ACL is specified, packets that are permitted by the uRPF ACL are forwarded in hardware and the denied packets are sent to the PISA for the uRPF check. This command enables hardware forwarding with the uRPF check for the packets that are denied by the uRPF ACL. However in this case packets permitted by uRPF ACL are sent to the PISA for forwarding.

uRPF is not supported on PVLAN host ports.

Examples

This example shows how to enable hardware uRPF when RPF and ACL are enabled:

```
Router(config)# mls ip cef rpf hw-enable-rpf-acl
Router(config)#
```

This example shows how to disable hardware uRPF when RPF and ACL are enabled:

```
Router(config)# no mls ip cef rpf hw-enable-rpf-acl
Router(config)#
```

Related Commands

Command	Description
ip verify unicast source reachable-via {any | rx}	Enables and configures RPF checks with ACL.

mls ip cef rpf interface-group

To define an interface group in the RPF-VLAN table, use the **mls ip cef rpf interface-group** command. To delete the interface group, use the **no** form of this command.

mls ip cef rpf interface-group *group-number interface1 interface2 interface3* [...]

no mls ip cef rpf interface-group *group-number interface1 interface2 interface3* [...]

Syntax Description

group-number	Interface group number; valid values are from 1 to 4.
interface	Interface number; see the "Usage Guidelines" section for formatting guidelines.
...	(Optional) Additional interface numbers; see the "Usage Guidelines" section for additional information.

Command Default

No groups are configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

A single interface group contains three to six interfaces. You can configure up to four interface groups. For each interface group, the first four entries are installed in the hardware RPF-VLAN table.

Enter the *interface* as *interface-typemod/port*.

Separate each interface entry with a space. You do not have to include a space between the *interface-type* and the *mod/port* arguments. See the "Examples" section for a sample entry.

Examples

This example shows how to define an interface group:

```
Router(config)# mls ip cef rpf interface-group 0 F2/1 F2/2 F2/3 F2/4 F2/5 F2/6
Router(config)#
```

mls ip cef rpf multipath

To configure the RPF modes, use the **mls ip cef rpf multipath** command. To return to the default settings, use the **no** form of this command.

mls ip cef rpf multipath {**interface-group** | **punt** | **pass**}

Syntax Description

interface-group	Disables the RPF check for packets coming from multiple path routes; see the "Usage Guidelines" section for additional information.
punt	Redirects the RPF-failed packets to the route processor for multiple path prefix support.
pass	Disables the RPF check for packets coming from multiple path routes.

Command Default

punt

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The interface-group mode is similar to the pass mode but utilizes the RPF_VLAN global table for the RPF check. Packets from other multiple path prefixes always pass the RPF check.

You enter the **mls ip cef rpf multipath interface-group** command to define an RPF_VLAN table interface group. One interface group contains from three to six interfaces, and you can configure up to four interface groups. For each interface group, the first four entries are installed in the hardware RPF_VLAN table. For the prefix that has more than three multiple paths, and all paths except two are part of that interface group, the FIB entry of that prefix uses this RPF_VLAN entry.

Examples

This example shows how to redirect the RPF-failed packets to the route processor for multiple path prefix support:

```
Router(config)# mls ip cef rpf multipath interface-group
Router(config)#
```

Related Commands

Command	Description
show mls cef ip	Displays the IP entries in the MLS-hardware Layer 3-switching table.

mls ip delete-threshold

To delete the configured ACL thresholds, use the **mls ip delete-threshold** command.

mls ip delete-threshold *acl-num*

Syntax Description

acl-num	Reflective ACL number; valid values are from 1 to 10000.

Command Default

This command has no default settings.

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

The **mls ip delete-threshold** command is active only when you enable the **mls ip reflexive ndr-entry tcam** command.

Examples

This example shows how to delete an ACL threshold:

```
Router(config)# mls ip delete-threshold 223
Router(config)#
```

Related Commands

Command	Description
mls ip install-threshold	Installs the configured ACL thresholds.
mls ip reflexive ndr-entry tcam	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.

mls ip directed-broadcast

To enable the hardware switching of the IP-directed broadcasts, use the **mls ip directed-broadcast** command. To return to the default settings, use the **no** form of this command.

mls ip directed-broadcast {**exclude-router** | **include-router**}

no mls ip directed-broadcast

Syntax Description

exclude-router	Forwards the IP-directed broadcast packet in the hardware to all hosts in the VLAN except the router.
include-router	Forwards the IP-directed broadcast packet in the hardware to all hosts in the VLAN including the router.

Command Modes

Disabled

Command Default

Interface configuration

Command History

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

Usage Guidelines

The **exclude-router** and **include-router** keywords both support hardware switching, but **exclude-router** does not send a copy of the hardware-switched packets to the router. If you enter the **include-router** keyword, the router does not forward the IP-directed broadcast packet again.

In the default mode, IP-directed broadcast packets are not forwarded in the hardware; they are handled at the process level by the PISA. The PISA decision to forward or not forward the packet is dependent on the **ip directed-broadcast** command configuration.

There is no interaction between the **ip directed-broadcast** command and the **mls ip directed-broadcast** command. The **ip directed-broadcast** command involves software forwarding, and the **mls ip directed-broadcast** command involves hardware forwarding.

MLS IP-directed broadcast supports a secondary interface address.

Any packets that hit the CPU are not forwarded unless you add the **ip directed-broadcast** command to the same interface.

You can configure the MLS IP-directed broadcasts on a port-channel interface but not on the physical interfaces on the port-channel interface. If you want to add a physical interface to a port-channel group, the physical interface cannot have the MLS IP-directed broadcast configuration. You have to first remove the configuration manually and then add the physical interface to the channel group. If a physical interface is already part of a channel group, the CLI will not accept the **mls ip directed-broadcast** configuration command on that physical interface.

Examples

This example shows how to forward the IP-directed broadcast packet in the hardware to all hosts in the VLAN with the exception of the router:

```
Router(config-if)# mls ip directed-broadcast exclude-router
Router(config-if)#
```

This example shows how to forward the IP-directed broadcast packet in the hardware to all hosts in the VLAN:

```
Router(config-if)# mls ip directed-broadcast include-router
Router(config-if)#
```

Related Commands

Command	Description
show mls cef adjacency	Displays hardware-switched IP-directed broadcast information.

mls ip inspect

To permit traffic through any ACLs that would deny the traffic through other interfaces, use the **mls ip inspect** command. To return to the default settings, use the **no** form of this command.

mls ip inspect *acl-name*

no mls ip inspect *acl-name*

Syntax Description

acl-name	ACL name.

Command Modes

Disabled

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

On a Catalyst 6500 series switch, when interfaces are configured to deny traffic, the CBAC permits traffic to flow bidirectionally only through the interface that is configured with the **ip inspect** command.

Examples

This example shows how to permit the traffic through a specific ACL (named deny_ftp_c):

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)#
```

Related Commands

Command	Description
ip inspect	Applies a set of inspection rules to an interface.

mls ip install-threshold

To install the configured ACL thresholds, use the **mls ip install-threshold** command.

mls ip install-threshold *acl-num*

Syntax Description

acl-num	Reflective ACL number; valid values are from 1 to 10000.

Command Modes

This command has no default settings.

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

The **mls ip install-threshold** command is active only when you enable the **mls ip reflexive ndr-entry tcam** command.

Examples

This example shows how to install an ACL threshold:

```
Router(config)# mls ip install-threshold 123
Router(config)#
```

Related Commands

Command	Description
mls ip delete-threshold	Deletes configured ACL thresholds.
mls ip reflexive ndr-entry tcam	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.

mls ip multicast (global configuration mode)

To enable MLS IP and configure the hardware switching globally, use the **mls ip multicast** command. To disable MLS IP, use the **no** form of this command.

mls ip multicast [**capability**]

mls ip multicast [**vrf** *name*] [**connected | egress local | mfd | refresh-state | shared-tree-mfd | threshold** *ppsec*]

no mls ip multicast [**vrf**]

Syntax Description

capability	(Optional) Exports the information about the egress capability from the switch processor to the route processor.
vrf *name*	(Optional) Specifies the VRF name.
connected	(Optional) Installs the interface/mask entries for bridging directly connected sources to the internal router.
egress local	(Optional) Populates the multicast expansion table with local Layer 3-routed interfaces.
mfd	(Optional) Enables complete hardware switching.
refresh-state	(Optional) Refreshes the expiration time of the (S,G) entry or the (*,G) entry with NULL OIF.
shared-tree-mfd	(Optional) Enables the complete shortcut for (*,G) flows.
threshold *ppsec*	(Optional) Sets the minimum traffic rate; below this rate, the flow is switched in the software instead of in the hardware. Valid values are from 10 to 10000 seconds.

Command Modes

The defaults are as follows:

- Multicast is disabled.
- Hardware switching is allowed for all eligible multicast routes.
- **connected** is enabled.
- **egress local** is disabled.
- **mfd** is enabled.
- **refresh-state** is enabled.
- **shared-tree-mfd** is enabled.

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

Note After you enter the **mls ip multicast egress local** command, you must perform a system reset for the configuration to take effect.

When entering the **mls ip multicast egress local** command, ensure that IPv6 multicast is not enabled. Since the egress multicast replication performance enhancement feature cannot separately turn on or turn off IPv4 and IPv6, you cannot have IPv4 and IPv6 multicast enabled when this feature is turned on.

These optional keywords are supported:

- **threshold**
- **connected**
- **refresh-state**
- **shared-tree-mfd**
- **mfd**

The **threshold** *ppsec* optional keyword and argument do not impact flows that are already populated in the hardware cache.

The expiration time refresh is updated when flow statistics are received from the Catalyst 6500 series switch (indicating that the traffic is received from the RPF interface).

Examples

This example shows how to enable the MLS IP shortcuts:

```
Router(config)# mls ip multicast
Router(config)#
```

This example shows how to enable the hardware switching on a specific multicast route:

```
Router(config)# mls ip multicast vrf test1
Router(config)#
```

This example shows how to export the information about egress capability from the switch processor to the route processor:

```
Router(config)# mls ip multicast capability
Router(config)#
```

This example shows how to populate the multicast expansion table with local Layer 3-routed interfaces:

```
Router(config)# mls ip multicast egress local
Router(config)#
```

Related Commands

Command	Description
mls rp ip (global configuration mode)	Enables external systems to establish IP shortcuts to the PISA.
show mls ip multicast	Displays the MLS IP information.

mls ip multicast (interface configuration mode)

To enable MLS IP shortcuts on the interface, use the **mls ip multicast** command. To disable MLS IP shortcuts on the interface, use the **no** form of this command.

mls ip multicast

no mls ip multicast

Syntax Description

This command has no arguments or keywords.

Command Modes

Multicast is disabled.

Command Default

Interface configuration

Command History

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

Examples

This example shows how to enable the MLS IP shortcuts:

```
Router(config-if)# mls ip multicast
Router(config-if)#
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.

mls ip multicast bidir gm-scan-interval

To set the RPF scan interval for the Bidir rendezvous point, use the **mls ip multicast bidir gm-scan-interval** command. To disable the RPF scan interval for the Bidir rendezvous point, use the **no** form of this command.

mls ip multicast bidir gm-scan-interval *interval*

no mls ip multicast bidir gm-scan-interval

Syntax Description

interval	RPF scan interval for the Bidir rendezvous point; valid values are from 1 to 1000 seconds.

Command Modes

10 seconds

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When you set the RPF scan interval for the Bidir rendezvous point, you set the time that the periodic scan timer updates the RPF in the DF table for all Bidir rendezvous points in the hardware.

Examples

This example shows how to set the RPF scan interval for the Bidir rendezvous point:

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

Related Commands

Command	Description
show mls ip multicast bidir	Displays the Bidir hardware-switched entries.

mls ip multicast connected

To enable the downloading of directly connected subnets globally, use the **mls ip multicast connected** command. To disable the downloading of directly connected subnets globally, use the **no** form of this command.

mls ip multicast connected

no mls ip multicast connected

Syntax Description

This command has no arguments or keywords.

Command Modes

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Do not create directly connected subnets for the following cases:

- To make more room available in the FIB TCAM
- The switch is the first-hop router for a source
- The entries are for Bidir, SSM, and DM mode groups

In these cases, if you enable the downloading of directly connected subnets, the directly connected source hits the MMLS (*,G) entry and is switched using the MMLS (*,G) entry. The registers are not sent to the route processor (in the case of PIM-SM), and the (S,G) state is not created on the first hop (in the case of PIM-DM).

The subnet entry is installed in the TCAM entries with a shorter mask to catch directly connected sources before they hit such entries. You can punt traffic from directly connected sources to the PISA. Once the PISA sees this traffic, it can install an MMLS (S,G) entry for this source, which gets installed before the subnet entry in the TCAM. New packets from this source are now switched with the (S,G) entry.

Examples

This example shows how to enable the downloading of directly connected subnets:

```
Router(config)# mls ip multicast connected
Router(config)#
```

Related Commands

Command	Description
mls ip multicast (global configuration mode)	Enables MLS IP and configures the hardware switching globally.
show mls ip multicast	Displays the MLS IP information.

mls ip multicast consistency-check

To enable and configure the hardware-shortcut consistency checker, use the **mls ip multicast consistency-check** command. To disable the consistency checkers, use the **no** form of this command.

mls ip multicast consistency-check [{**settle-time** *seconds*} | {**type scan-mroute** [**count** *count-number*] | {**settle-time** *seconds*}} | {**period** *seconds*}]

no mls ip multicast consistency-check

Syntax Description

settle-time *seconds*	(Optional) Specifies the settle time for entry/oif for the consistency checker; valid values are from 2 to 3600 seconds.
type scan-mroute	(Optional) Specifies the type of consistency check as a scan check of the mroute table.
count *count-number*	(Optional) Specifies the maximum number of prefixes to check per scan; valid values are from 2 to 500.
period *seconds*	(Optional) Specifies the period between scans; valid values are from 2 to 3600 seconds.

Command Default

The defaults are as follows:

- Consistency check is enabled.
- **count** *count-number* is **20**.
- **period** *seconds* is **2** seconds.
- **settle-time** *seconds* is **60** seconds.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The *oif* entry is the outgoing interface of a multicast {*,G} or {source, group} flow.

The consistency checker scans the mroute table and assures that the multicast-hardware entries are consistent with the mroute table. Whenever an inconsistency is detected, the inconsistency is automatically corrected.

To display the inconsistency error, use the **show mls ip multicast consistency-check** command.

Examples

This example shows how to enable the hardware-shortcut consistency checker:

```
Router (config)# mls ip multicast consistency-check
Router (config)#
```

This example shows how to enable the hardware-shortcut consistency checker and configure the scan check of the mroute table:

```
Router (config)# mls ip multicast consistency-check type scan-mroute count 20 period 35
Router (config)#
```

This example shows how to enable the hardware-shortcut consistency checker and specify the period between scans:

```
Router (config)# mls ip multicast consistency-check type scan-mroute period 35
Router (config)#
```

Related Commands

Command	Description
show mls ip multicast consistency-check	Displays the MLS IP information.

mls ip multicast flow-stat-timer

To set the time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor, use the **mls ip multicast flow-stat-timer** command. To return to the default settings, use the **no** form of this command.

mls ip multicast flow-stat-timer *num*

no mls ip multicast flow-stat-timer

Syntax Description

num	Time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor.

Command Default

25 seconds

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to configure the time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor:

```
Router (config)# mls ip multicast flow-stat-timer 10
Router (config)#
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.

mls ip multicast replication-mode

To enable and specify the replication mode, use the **mls ip multicast replication-mode** command. To restore the system to automatic detection mode, use the **no** form of this command.

mls ip multicast replication-mode {**egress** | **ingress**}

no mls ip multicast replication-mode {**egress** | **ingress**}

Syntax Description

egress	Forces the system to the egress mode of replication.
ingress	Forces the system to the ingress mode of replication.

Command Default

ingress

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The Supervisor Engine 32 PISA does not support the **egress** keyword.

Note During the change from egress- to ingress-replication mode, traffic interruptions may occur because the shortcuts are purged and reinstalled. To avoid interruptions in traffic forwarding, enter the **mls ip multicast replication-mode ingress** command.

If you enter the **no mls ip multicast replication-mode ingress** command, only the forced-ingress mode resets

Examples

This example shows how to enable the ingress-replication mode:

```
Router (config)# mls ip multicast replication-mode ingress
Router (config)#
```

Related Commands

Command	Description
show mls ip multicast capability	Displays the MLS IP information.

mls ip multicast sso

To configure the SSO parameters, use the **mls ip multicast sso** command. To return to the default settings, use the **no** form of this command.

mls ip multicast sso {{**convergence-time** *time*} | {**leak** *interval*} | {**leak** *percentage*}}

Syntax Description

convergence-time *time*	Specifies the maximum time to wait for protocol convergence; valid values are from 0 to 3600 seconds.
leak *interval*	Specifies the packet-leak interval; valid values are from 0 to 3600 seconds.
leak *percentage*	Specifies the percentage of multicast packets leaked to the router during switchover so that protocol convergence can take place; valid values are from 1 to 100 percent.

Command Default

The defaults are as follows:

- **convergence-time** *time*—20 seconds
- **leak** *interval*—60 seconds
- **leak** *percentage*—10 percent

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to set the maximum time to wait for protocol convergence:

```
Router (config)# mls ip multicast sso convergence-time 300
Router (config)#
```

This example shows how to set the packet-leak interval:

```
Router (config)# mls ip multicast sso leak 200
Router (config)#
```

This example shows how to set the packet-leak percentage:

```
Router (config)# mls ip multicast sso leak 55
Router (config)#
```

Related Commands

Command	Description
show mls ip multicast sso	Displays information about multicast high-availability SSO.

mls ip multicast stub

To enable the support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **mls ip multicast stub** command. To disable support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **no** form of this command.

mls ip multicast stub

no mls ip multicast stub

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **mls ip multicast stub** command, creates the following filters on a routed interface or a VLAN:

- Permits IP packets from all addresses that are connected to the interface to any IP destination. An address is connected to the interface if it is within the IP address prefixes configured through the **ip address** *addr mask* [**secondary**] command.

  This filter is meant to permit unicast and multicast packets from directly connected sources.

- Permits IP multicast packets from any source address to multicast group prefixes 224.0.0.0/24 and 224.0.1.0/24.

  This filter allows packets to be sent from any source address to well-known multicast addresses; 224.0.0.0/24 is used by protocols such as PIM, OSPF, EIGRP, or NTP. Addresses in 224.0.1.0/24 are used by protocols such as AutoRP (224.0.1.39, 224.0.1.40).

- Denies any other IP multicast packets.

  This deny filter is meant to inhibit any multicast packets from nondirectly connected sources and is applied to the packets received on this interface or VLAN.

The permit IP multicast packets and the deny any other IP multicast packets filters are the same for all interface or VLANs to which you configure the **mls ip multicast stub** command. The permit IP packets from all addresses that are connected to the interface to any IP destination filter is different for each interface or VLAN.

Examples

This example shows how to enable the support for the non-RPF traffic drops for the PIM sparse-mode stub networks:

```
Router(config-if)# mls ip multicast stub
Router(config-if)#
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.

mls ip multicast threshold

To configure a threshold rate for installing hardware shortcuts, use the **mls ip multicast threshold** command. To deconfigure the threshold, use the **no** form of this command.

mls ip multicast threshold *ppsec*

no mls ip multicast threshold

Syntax Description

ppsec	Threshold in packets per seconds; valid values are from 10 to 10000 packets per second.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to prevent creation of MLS entries for short-lived multicast flows such as join requests.

If multicast traffic drops below the configured multicast rate threshold, all multicast traffic is routed by the PISA.

This command does not affect already installed routes. For example, if you enter this command and the shortcuts are already installed, the shortcuts are not removed if they are disqualified. To apply the threshold to existing routes, clear the route and let it reestablish.

Examples

This example shows how to configure the IP MLS threshold to 10 packets per second:

```
Router (config)# mls ip multicast threshold 10
Router (config)#
```

Related Commands

Command	Description
mls rp ip (global configuration mode)	Enables external systems to establish IP shortcuts to the PISA.
show mls ip multicast	Displays the MLS IP information.

mls ip nat netflow-frag-l4-zero

To zero out the Layer 4 information in the NetFlow lookup table for fragmented packets, use the **mls ip nat netflow-frag-l4-zero** command.

mls ip nat netflow-frag-l4-zero

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

Use the **mls ip nat netflow-frag-l4-zero** command to prevent matching the first fragment to the NetFlow shortcut (normal operation) that is sent to the software. The next fragments that are sent to the software are translated based on the Layer 4 port information from the first fragment. The translation based on the Layer 4 port information from the first fragment occurs because there are no fragment bits for matching in the NetFlow key.

When there is a large feature configuration on an interface that requires a large number of ACL TCAM entries/masks that are programmed in TCAM, if the interface is configured as a NAT-inside interface, the feature configuration may not fit in the ACL TCAM and the traffic on the interface may get switched in the software.

Examples

This example shows how to zero out the Layer 4 information in the NetFlow lookup table for fragmented packets:

```
Router (config)# mls ip nat netflow-frag-l4-zero
Router (config)#
```

mls ip pbr

To enable the MLS support for policy-routed packets, use the **mls ip pbr** command. To disable the MLS support for policy-routed packets, use the **no** form of this command.

mls ip pbr [**null0**]

no mls ip pbr

Syntax Description

null0	(Optional) Enables the hardware support for the interface null0 in the route maps.

Command Default

MLS support for policy-routed packets is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Note Do not enable PBR and SLB on the same interface; PBR-based packets are not forwarded correctly.

When you enable the hardware-policy routing by entering the **mls ip pbr** command, all policy routing occurs in the hardware and is applied to all interfaces, regardless of which interface was configured for policy routing.

Use the **null0** keyword when you have routed traffic only to enable the hardware support for the **set interface null0** in the route maps.

Examples

This example shows how to enable the MLS support for policy-routed packets:

```
Router(config)# mls ip pbr
Router(config)#
```

Related Commands

Command	Description
show tcam interface vlan acl	Displays information about the interface-based TCAM.

mls ip reflexive ndr-entry tcam

To enable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR, use the **mls ip reflexive ndr-entry tcam** command. To disable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR, use the **no** form of this command.

mls ip reflexive ndr-entry tcam

no mls ip reflexive ndr-entry tcam

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When you enter the **mls ip reflexive ndr-entry tcam** command, the reflexive ACL dynamic entries are installed in TCAM instead of in NetFlow.

Examples

This example shows how to enable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR:

```
Router(config)# mls ip reflexive ndr-entry tcam
Router(config)#
```

This example shows how to disable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR:

```
Router(config)# no mls ip reflexive ndr-entry tcam
Router(config)#
```

Related Commands

Command	Description
mls ip delete-threshold	Deletes the configured ACL thresholds.
mls ip install-threshold	Installs the configured ACL thresholds.

mls ipv6 acl compress address unicast

To turn on the compression of IPv6 addresses, use the **mls ipv6 acl compress address unicast** command. To turn off the compression of IPv6 addresses, use the **no** form of this command.

mls ipv6 acl compress address unicast

no mls ipv6 acl compress address unicast

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Caution Do not enable the compression mode if you have noncompressible address types in your network. A list of compressible address types and the address compression methosd are listed in Table 2-15.

Table 2-15 Compressible Address Types and Methods

Address Type	Compression Method
EUI-64 based on MAC address	This address is compressed by removing 16 bits from bit locations [39:24]. No information is lost when the hardware compresses these addresses.
Embedded IPv4 address	This address is compressed by removing the upper 16 bits. No information is lost when the hardware compresses these addresses.

Table 2-15 Compressible Address Types and Methods (continued)

Address Type	Compression Method
Link Local	These addresses are compressed by removing the zeros in bits [95:80] and are identified using the same packet type as the embedded IPv4 address. No information is lost when the hardware compresses these addresses.
Others	If the IPv6 address does not fall into any of the above categories, it is classified as other. If the IPv6 address is classified as other, the following occurs: • If the compress mode is on, the IPv6 address is compressed similarly to the EUI-64 compression method (removal of bits [39:24]) to allow for the Layer 4 port information to be used as part of the key used to look up the QoS TCAM, but Layer 3 information is lost. • If the global compression mode is off, the entire 128 bits of the IPv6 address are used. The Layer 4 port information cannot be included in the key to look up the QoS TCAM because of the size constraints on the IPv6 lookup key.

Examples

This example shows how to turn on the compression of the noncompressible IPv6 addresses:

```
Router(config)# mls ipv6 acl compress address unicast
Router(config)#
```

This example shows how to turn off the compression of the noncompressible IPv6 addresses:

```
Router(config)# no mls ipv6 acl compress address unicast
Router(config)#
```

Related Commands

Command	Description
show fm ipv6 traffic-filter	Displays the IPv6 information.
show mls netflow ipv6	Displays configuration information about the NetFlow hardware.

mls ipv6 acl source

To deny all IPv6 packets from a source-specific address, use the **mls ipv6 acl source** command. To accept all IPv6 packets from a source-specific address, use the **no** form of this command.

mls ipv6 acl source {**loopback** | **multicast**}

no mls ipv6 acl source {**loopback** | **multicast**}

Syntax Description

loopback	Denies all IPv6 packets with a source loopback address.
multicast	Denies all IPv6 packets with a source multicast address.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to deny all IPv6 packets with a source loopback address:

```
Router(config)# mls ipv6 acl source loopback
Router(config)#
```

This example shows how to deny all IPv6 packets with a source multicast address:

```
Router(config)# no mls ipv6 acl source multicast
Router(config)#
```

Related Commands

Command	Description
show mls netflow ipv6	Displays configuration information about the NetFlow hardware.

mls mpls (recirculation)

To enable MPLS recirculation, use the **mls mpls** command. To disable MPLS recirculation, use the **no** form of this command.

mls mpls {**recir-agg** | **tunnel-recir**}

no mls mpls {**recir-agg** | **tunnel-recir**}

Syntax Description

recir-agg	Recirculates the MPLS aggregated-label packets (new aggregated labels are impacted only).
tunnel-recir	Recirculates the tunnel-MPLS packets.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that need to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Catalyst 6500 series switch.

Use the **show erm statistics** command to display the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

Examples

This example shows how to enable the aggregated-label MPLS recirculation:

```
Router(config)# mls mpls recir-agg
Router(config)#
```

This example shows how to enable the tunnel-MPLS recirculation:

```
Router(config)# mls mpls tunnel-recir
Router(config)#
```

This example shows how to disable the aggregated-label MPLS recirculation:

```
Router(config)# no mls mpls recir-agg
Router(config)#
```

This example shows how to disable the tunnel-MPLS recirculation:

```
Router(config)# no mls mpls tunnel-recir
Router(config)#
```

Related Commands

Command	Description
show erm statistics	Displays the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

mls mpls (guaranteed bandwidth traffic engineering)

To configure the guaranteed bandwidth traffic engineering flow parameters globally, use the **mls mpls** command. To return to the default settings, use the **no** form of this command.

mls mpls {{**gb-te-burst** *burst*} | {**gb-te-cir-ratio** *ratio*} | {**gb-te-dscp** *dscp-value* [**markdown**]} | {**gb-te-enable** [**global-pool**]}}

no mls mpls {{**gb-te-burst** *burst*} | {**gb-te-cir-ratio** *ratio*} | {**gb-te-dscp** *dscp-value* [**markdown**]} | {**gb-te-enable** [**global-pool**]}}

Syntax Description

gb-te-burst *burst*	Specifies the burst duration for the guaranteed bandwidth traffic engineering flows; valid values are from 100 to 30000 milliseconds.
gb-te-cir-ratio *ratio*	Specifies the ratio for the committed information rate policing; valid values are from 1 to 100 percent.
gb-te-dscp *dscp-value*	Specifies the DSCP map for the guaranteed bandwidth traffic engineering flows; valid values are from 0 to 63.
markdown	(Optional) Marks down or drops the nonconforming flows.
gb-te-enable	Enables the guaranteed bandwidth traffic engineering flow policing.
global-pool	(Optional) Specifies using resources allocated from the global pool to the police traffic engineering flows.

Command Default

The default settings are as follows:

- *burst* is 1000 milliseconds.
- *ratio* is 1 percent.
- *dscp-value* is 40.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **mls qos map dscp-exp** command to reset the Exp value of the MPLS packet when the out-label gets swapped.

If you do not enable tunnel-MPLS recirculation, the IPv4 and IPv4-tunneled packets that need to be labeled (for example, the packets that are encapsulated with an MPLS header) will be corrupted when they are transmitted from the Catalyst 6500 series switch.

Use the **show erm statistics** command to display the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

Examples

This example shows how to specify the burst duration for the guaranteed bandwidth traffic engineering flows:

```
Router(config)# mls mpls gb-te-burst 2000
Router(config)#
```

This example shows how to specify the ratio for CIR policing:

```
Router(config)# mls mpls gb-te-ratio 30
Router(config)#
```

This example shows how to specify the DSCP map for the guaranteed bandwidth traffic engineering flows and to drop the nonconforming flows:

```
Router(config)# mls mpls gb-te-dscp 25 markdown
Router(config)#
```

This example shows how to enable the guaranteed bandwidth traffic engineering flow policing:

```
Router(config)# mls mpls gb-te-enable
Router(config)#
```

Related Commands

Command	Description
show erm statistics	Displays the FIB TCAM exception status for IPv4, IPv6, and MPLS protocols.

mls nde flow

To specify the filter options for NDE, use the **mls nde flow** command. To clear the NDE flow filter and reset the filter to the default settings, use the **no** form of this command.

mls nde flow {**include** | **exclude**} {{**dest-port** *port-num*} | {**destination** *ip-addr ip-mask*} | {**protocol** {**tcp** | **udp**}} | {**source** *ip-addr ip-mask*} | {**src-port** *port-num*}}

no mls nde flow {**include** | **exclude**}

Syntax Description

include	Allows importing of all flows except the flows matching the given filter.
exclude	Allows exporting of all flows matching the given filter.
dest-port *port-num*	Specifies the destination port to filter; valid values are from 1 to 100.
destination *ip-addr ip-mask*	Specifies a destination IP address and mask to filter.
protocol	Specifies the protocol to include or exclude.
tcp	Includes or excludes TCP.
udp	Includes or excludes UDP.
source *ip-addr ip-mask*	Specifies a source IP address and subnet mask bit to filter.
src-port *port-num*	Specifies the source port to filter.

Command Default

The defaults are as follows:

- All expired flows are imported.
- Interface export is disabled (**no mls nde interface**).

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **mls nde flow** command adds filtering to the NDE. The expired flows matching the specified criteria are exported. These values are stored in NVRAM and do not clear when NDE is disabled. If any option is not specified in this command, it is treated as a wildcard. The NDE filter in NVRAM does not clear when you disable NDE.

Only one filter can be active at a time. If you do not enter the **exclude** or **include** keyword, the filter is assumed to be an inclusion filter.

The include and exclude filters are stored in NVRAM and are not removed if you disable NDE.

ip-addr maskbits is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.25.2.1/22 indicates a 22-bit subnet address. The *ip-addr* is a full host address, such as 193.22.253.1/22.

Examples

This example shows how to specify an interface flow filter so that only expired flows to destination port 23 are exported (assuming that the flow mask is set to ip-flow):

```
Router(config)# mls nde flow include dest-port 23
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls nde interface

To populate the additional fields in the NDE packets, use the **mls nde interface** command. To disable the population of the additional fields, use the **no** form of this command.

mls nde interface

no mls nde interface

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can configure NDE to populate the following additional fields in the NDE packets:

- Egress interface SNMP index
- Source-autonomous system number
- Destination-autonomous system number
- IP address of the next-hop router

The ingress-interface SNMP index is always populated if the flow mask is interface-full or interface-src-dst.

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

Examples

This example shows how to populate the additional fields in the NDE packets:

```
Router(config)# mls nde interface
Router(config)#
```

This example shows how to disable the population of the additional fields:

```
Router(config)# no mls nde interface
Router(config)#
```

Related Commands

Command	Description
mls netflow	Enables NetFlow to gather statistics.
mls netflow sampling	Enables the sampled NetFlow on an interface.

mls nde sender

To enable MLS NDE export, use the **mls nde sender** command. To disable MLS NDE export, use the **no** form of this command.

mls nde sender [**version** *version*]

no mls nde sender

Syntax Description

version *version*	(Optional) Specifies the NDE version; valid values are **5** and **7**.

Command Default

The defaults are as follows:

- MLS NDE export is disabled.
- *version* is **7**.

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to enable MLS NDE export:

```
Router(config)# mls nde sender
Router(config)#
```

This example shows how to disable MLS NDE export:

```
Router(config)# no mls nde sender
Router(config)#
```

Related Commands

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

mls netflow

To enable NetFlow to gather the statistics, use the **mls netflow** command. To disable NetFlow from gathering the statistics, use the **no** form of this command.

mls netflow

no mls netflow

Syntax Description

interface	(Optional) Specifies statistics gathering per interface.

Command Default

Enabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

NetFlow gathers the statistics from traffic that flows through the Catalyst 6500 series switch and stores the statistics in the NetFlow table. You can gather the statistics globally based on a protocol or optionally per interface.

If you are not using NDE or the Cisco IOS features that use the hardware NetFlow table (micro-flow QoS, WCCP, TCP Intercept, or Reflexive ACLs), you may safely disable the use and maintenance of the hardware NetFlow table using the **no mls netflow** command in global configuration mode.

Examples

This example shows how to gather the statistics:

```
Router(config)# mls netflow
Router(config)#
```

This example shows how to disable NetFlow from gathering the statistics:

```
Router(config)# no mls netflow
Disabling MLS netflow entry creation.
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls netflow maximum-flows

To configure the maximum flow allocation in the NetFlow table, use the **mls netflow maximum-flows** command. To return to the default settings, use the **no** form of this command.

mls netflow maximum-flows [*maximum-flows*]

no mls netflow maximum-flows

Syntax Description

maximum-flows	(Optional) Maximum number of flows; valid values are **16**, **32**, **64**, **80**, **96**, and **128**. See the "Usage Guidelines" section for additional information.

Command Default

128

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The value that you specify for the maximum number of flows is that value times 1000. For example, if you enter 32, you specify that 32,000 is the maximum number of permitted flows.

Examples

This example shows how to configure the maximum flow allocation in the NetFlow table:

```
Router(config)# mls netflow maximum-flows 96
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls netflow maximum-flows
Router(config)#
```

Related Commands

Command	Description
show mls netflow table-contention	Displays configuration information at the table contention level for the NetFlow hardware.

mls netflow sampling

To enable the sampled NetFlow on an interface, use the **mls netflow sampling** command. To disable the sampled NetFlow, use the **no** form of this command.

mls netflow sampling

no mls netflow sampling

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

To enable sampling, you must enter the **mls sampling** command and the **mls netflow sampling** command on the appropriate interfaces. If you do not enter the **mls netflow sampling** command, NDE will not export flows.

Depending on the current flow mask, the sampled NetFlow can be global or per interface. For Interface-Full and Interface-Src-Dest flow masks, the sampled NetFlow is enabled on a per-interface basis. For all the other flow masks, the sampled NetFlow is always global and turned on/off for all interfaces.

Enter the **mls sampling** command to enable the sampled NetFlow globally.

Examples

This example shows how to enable the sampled NetFlow on an interface:

```
Router(config-if)# mls netflow sampling
Router(config-if)#
```

This example shows how to disable the sampled NetFlow on an interface:

```
Router(config-if)# no mls netflow sampling
Router(config-if)#
```

Related Commands

Command	Description
mls sampling	Enables the sampled NetFlow and specifies the sampling method.
show mls sampling	Displays information about the sampled NDE status.

mls netflow usage notify

To monitor the NetFlow table usage on the switch processor, use the **mls netflow usage notify** command. To return to the default settings, use the **no** form of this command.

mls netflow usage notify {*threshold interval*}

no mls netflow usage notify

Syntax Description

threshold	Percentage threshold that, if exceeded, displays a warning message; valid values are from 20 to 100 percent.
interval	Frequency that the NetFlow table usage is checked; valid values are from 120 to 1000000 seconds.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If the NetFlow table usage monitoring is enabled and the NetFlow table usage exceeds the percentage threshold, a warning message is displayed.

NetFlow gathers statistics from traffic that flows through the Catalyst 6500 series switch and stores the statistics in the NetFlow table. You can gather statistics globally based on a protocol or optionally per interface.

If you are not using NDE or the Cisco IOS features that use the hardware NetFlow table (micro-flow QoS, WCCP, TCP Intercept, or Reflexive ACLs), you may safely disable the use and maintenance of the hardware NetFlow table using the **no mls netflow** command in global configuration mode.

Examples

This example shows how to configure the monitoring of the NetFlow table usage on the switch processor:

```
Router(config)# mls netflow usage notify 80 300
Router(config)#
```

Related Commands

Command	Description
show mls netflow usage	Displays configuration information about the NetFlow hardware.

mls qos (global configuration mode)

To enable the QoS functionality globally, use the **mls qos** command. To disable the QoS functionality globally, use the **no** form of this command.

mls qos

no mls qos

Syntax Description

This command has no arguments or keywords.

Command Default

QoS is globally disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you enable QoS globally, QoS is enabled on all interfaces with the exception of the interfaces where you disabled QoS. If you disable QoS globally, all traffic is passed in QoS pass-through mode.

In port-queueing mode, PFC QoS (marking and policing) is disabled, and packet ToS and CoS are not changed by the PFC. All queueing on rcv and xmt is based on a QoS tag in the incoming packet, which is based on the incoming CoS.

For 802.1Q or ISL-encapsulated port links, queueing is based on the packet 802.1Q or ISL CoS.

For the router main interfaces or access ports, queueing is based on the configured per-port CoS (the default CoS is 0).

This command enables or disables TCAM QoS on all interfaces that are set in the OFF state.

Examples

This example shows how to enable QoS globally:

```
Router(config)# mls qos
Router(config)#
```

This example shows how to disable QoS globally on the Catalyst 6500 series switch:

```
Router(config)# no mls qos
Router(config)#
```

Related Commands

Command	Description
mls qos (interface configuration mode)	Enables the QoS functionality on an interface.
show mls qos	Displays MLS QoS information.

mls qos (interface configuration mode)

To enable the QoS functionality on an interface, use the **mls qos** command. To disable QoS functionality on an interface, use the **no** form of this command.

mls qos

no mls qos

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Although the CLI allows you to configure PFC-based QoS on the WAN ports on the OC-12 ATM OSMs and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs.

If you disable QoS globally, it is also disabled on all interfaces.

This command enables or disables TCAM QoS (classification, marking, and policing) for the interface.

Examples

This example shows how to enable QoS on an interface:

```
Router(config-if)# mls qos
Router(config-if)#
```

Related Commands

Command	Description
mls qos (global configuration mode)	Enables the QoS functionality globally.
show mls qos	Displays MLS QoS information.

mls qos aggregate-policer

To define a named aggregate policer for use in policy maps, use the **mls qos aggregate-policer** command. This policer can be shared by different policy map classes and on different interfaces. To delete a named aggregate policer, use the **no** form of this command.

mls qos aggregate-policer *name rate-bps*

mls qos aggregate-policer *name rate-bps burst-bytes maximum-burst-bytes*

mls qos aggregate-policer *name rate-bps* [{**conform-action** {**drop** [**exceed-action** *action*]}} | {**set-dscp-transmit** [*new-dscp*]} | {**set-prec-transmit** [*new-precedence*]} | {**transmit** [{**exceed-action** *action*} | {**violate-action** *action*]}}

mls qos aggregate-policer *aggregate-name rate-bps* {**pir** *peak-rate-bps* [{**conform-action** {**drop** [**exceed-action** *action*]}} | {**set-dscp-transmit** [*new-dscp*]} | {**set-prec-transmit** [*new-precedence*]} | {**transmit** [{**exceed-action** *action*}} | {**violate-action** *action*}]]}

no mls qos aggregate-policer *name*

Syntax Description

name	Name of the aggregate policer.
rate-bps	Maximum bits per second; valid values are from 32000 to 10000000000.
burst-bytes	Burst bytes; valid values are from 1000 to 31250000.
maximum-burst-bytes	Maximum burst bytes; valid values are from 1000 to 31250000 (if entered, must be set equal to normal-burst-bytes).
conform-action	(Optional) Specifies the action to be taken when the rate is not exceeded.
drop	(Optional) Drops the packet.
exceed-action *action*	(Optional) Specifies the action to be taken when QoS values are exceeded; see the "Usage Guidelines" section for valid values.
set-dscp-transmit	Sets the DSCP value and sends the packet.
new-dscp	(Optional) New DSCP value; valid values are from 0 to 63.
set-prec-transmit	Rewrites packet precedence and sends the packet.
new-precedence	(Optional) New precedence value; valid values are from 0 to 7.
violate-action *action*	(Optional) Specifies the action to be taken when QoS values are violated; see the "Usage Guidelines" section for valid values.
pir *peak-rate-bps*	Sets the PIR peak rate; valid values are from 32000 to 10000000000.

Command Default

The defaults are as follows:

- *extended-burst-bytes* is equal to *burst-bytes*.
- **conform-action** is **transmit**.
- **exceed-action** is **drop**.
- **violate-action** is equal to the **exceed-action**.
- **pir** *peak-rate-bps* is equal to the normal (**cir**) rate.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Valid values for *action* are as follows:

- **drop**—Drops the packet
- **policed-dscp-transmit**—Changes the DSCP per the policed-DSCP map and sends it
- **transmit**—Transmits the package

The Catalyst 6500 series switch supports up to 1023 aggregates and 1023 policing rules.

The **mls qos aggregate-policer** command allows you to configure an aggregate flow and a policing rule for that aggregate. When you enter the rate and burst parameters, the range for the average rate is 32 Kbps to 4 Gbps (entered as 32000 and 4000000000) and the range for the burst size is 1 KB (entered as 1000) to 512 MB (entered as 512000000). Modifying an existing aggregate rate limit entry causes that entry to be modified in NVRAM and in the Catalyst 6500 series switch if that entry is currently being used.

Note Due to hardware granularity, the rate value is limited so the burst that you configure may not be the value that is used.

Modifying an existing microflow or aggregate rate limit modifies that entry in NVRAM and in the Catalyst 6500 series switch if it is currently being used.

When you enter the aggregate policer 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 alphabetic 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**

Examples

This example shows how to configure a QoS aggregate policer to allow a maximum of 100000 bits per second with a normal burst byte size of 10000, set DSCP to 48 when these rates are not exceeded, and drop packets when these rates are exceeded:

```
Router(config)# mls qos aggregate-policer micro-one 100000 10000 conform-action set-dscp
48 exceed action drop
Router(config)#
```

Related Commands

Command	Description
set ip dscp (policy-map configuration)	Marks a packet by setting the IP DSCP in the ToS byte.

mls qos bridged

To enable the microflow policing for bridged traffic on Layer 3 LAN interfaces, use the **mls qos bridged** command. To disable microflow policing for bridged traffic, use the **no** form of this command.

mls qos bridged

no mls qos bridged

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is supported on SVIs only.

Examples

This example shows how to enable the microflow policing for bridged traffic on a VLAN interface:

```
Router(config-if)# mls qos bridged
Router(config-if)#
```

Related Commands

Command	Description
show mls qos	Displays MLS QoS information.

mls qos channel-consistency

To enable the QoS-port attribute checks on EtherChannel bundling, use the **mls qos channel-consistency** command. To disable the QoS-port attribute checks on EtherChannel bundling, use the **no** form of this command.

mls qos channel-consistency

no mls qos channel-consistency

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **mls qos channel-consistency** command is supported on port channels only.

Examples

This example shows how to enable the QoS-port attribute checks on the EtherChannel bundling:

```
Router(config-if)# mls qos channel-consistency
Router(config-if)#
```

This example shows how to disable the QoS-port attribute checks on the EtherChannel bundling:

```
Router(config-if)# no mls qos channel-consistency
Router(config-if)#
```

mls qos cos

To define the default CoS value for an interface, use the **mls qos cos** command. To remove a prior entry, use the **no** form of this command.

mls qos cos *cos-value*

no mls qos cos *cos-value*

Syntax Description

cos-value	Default CoS value for the interface; valid values are from 0 to 7.

Command Default

The defaults are as follows:

- *cos-value* is **0**.
- CoS override is not configured.

Command Default

Interface configuration

Command History

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

Usage Guidelines

CoS values are configurable on physical LAN ports only.

Examples

This example shows how to configure the default QoS CoS value as 6:

```
Router(config-if)# mls qos cos 6
Router(config-if)#
```

Related Commands

Command	Description
show mls qos	Displays MLS QoS information.

mls qos cos-mutation

To attach an ingress-CoS mutation map to the interface, use the **mls qos cos-mutation** command. To remove the ingress-CoS mutation map from the interface, use the **no** form of this command.

mls qos cos-mutation *cos-mutation-table-name*

no mls qos cos-mutation

Syntax Description

cos-mutation-table-name	Name of the ingress-CoS mutation table.

Command Modes

No table is defined.

Command Default

Interface configuration

Command History

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

Examples

This example shows how to attach the ingress-CoS mutation map named mutemap2:

```
Router(config-if)# mls qos cos-mutation mutemap2
Router(config-if)#
```

Related Commands

Command	Description
mls qos map cos-mutation	Maps a packet's CoS to a new CoS value.
show mls qos	Displays MLS QoS information.

mls qos dscp-mutation

To attach an egress-DSCP mutation map to the interface, use the **mls qos dscp-mutation** command. To remove the egress-DSCP mutation map from the interface, use the **no** form of this command.

mls qos dscp-mutation *dscp-mutation-table-name*

no mls qos dscp-mutation

Syntax Description

dscp-mutation-table-name	Name of the egress-DSCP mutation table.

Command Modes

No table is defined.

Command Default

Interface configuration

Command History

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

Examples

This example shows how to attach the egress-DSCP mutation map named mutemap1:

```
Router(config-if)# mls qos dscp-mutation mutemap1
Router(config-if)#
```

Related Commands

Command	Description
mls qos map dscp-mutation	Defines a named DSCP mutation map.
show mls qos	Displays MLS QoS information.

mls qos exp-mutation

To attach an egress-EXP mutation map to the interface, use the **mls qos exp-mutation** command. To remove the egress-EXP mutation map from the interface, use the **no** form of this command.

mls qos exp-mutation *exp-mutation-table-name*

no mls qos exp-mutation

Syntax Description

exp-mutation-table-name	Name of the egress-EXP mutation table.

Command Default

No table is defined.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to attach the egress-exp mutation map named mutemap2:

```
Router(config-if)# mls qos exp-mutation mutemap2
Router(config-if)#
```

Related Commands

Command	Description
mls qos map dscp-mutation	Defines a named DSCP mutation map.
show mls qos mpls	Displays an interface summary for MPLS QoS classes in the policy maps.

mls qos loopback

To remove a router port from the SVI flood for VLANs that are carried through by the loopback cable, use the **mls qos loopback** command. To return to the default settings, use the **no** form of this command.

mls qos loopback

no mls qos loopback

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Default

Interface configuration

Command History

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

Usage Guidelines

With **mls qos loopback** applied at the interface, the packets are not forwarded to the destination.

Before you enter the **mls qos loopback** command, you must specify a MAC address for the OSM interface. The MAC address must be different from the LAN router MAC address that is used in PFC2 hardware switching.

Examples

This example shows how to prevent packets from being forwarded to the destination:

```
Router (config-if)# mls qos loopback
Router (config-if)#
```

mls qos map cos-dscp

To define the ingress CoS-to-DSCP map for trusted interfaces, use the **mls qos map cos-dscp** command. To remove a prior entry, use the **no** form of this command.

mls qos map cos-dscp *values*

no mls qos map cos-dscp

Syntax Description

values	Eight DSCP values, separated by spaces, corresponding to the CoS values; valid values are from 0 to 63.

Command Modes

The default CoS-to-DSCP configuration is listed in Table 2-16.

Table 2-16 CoS-to-DSCP Default Map

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

The CoS-to-DSCP map is used to map the CoS of packets arriving on trusted interfaces (or flows) to a DSCP where the trust type is trust-cos. This map is a table of eight CoS values (0 through 7) and their corresponding DSCP values. The Catalyst 6500 series switch has one map.

Examples

This example shows how to configure the ingress CoS-to-DSCP map for trusted interfaces:

```
Router(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Router(config)#
```

Related Commands

Command	Description
mls qos map dscp-cos	Defines an egress DSCP-to-CoS map.
mls qos map ip-prec-dscp	Defines an ingress-IP precedence-to-DSCP map for trusted interfaces.
mls qos map policed-dscp	Sets the mapping of policed DSCP values to marked-down DSCP values.
show mls qos maps	Displays information about the QoS map configuration and run-time version.

mls qos map cos-mutation

To map a packet's CoS to a new CoS value, use the **mls qos map cos-mutation** command. To remove the map, use the **no** form of this command.

mls qos map cos-mutation *name mutated_cos1 mutated_cos2 mutated_cos3 mutated_cos4 mutated_cos5 mutated_cos6 mutated_cos7 mutated_cos8*

no mls qos map cos-mutation *name*

Syntax Description

name	Name of the CoS map.
mutated_cos1 … *mutated_cos8*	Eight CoS out values, separated by spaces; valid values are from 0 to 7. See the "Usage Guidelines" section for additional information.

Command Modes

If the CoS-to-CoS mutation map is not configured, the default CoS-to-CoS mutation mapping is listed in Table 2-17.

Table 2-17 CoS-to-CoS Default Map

CoS-in	0	1	2	3	4	5	6	7
CoS-out	0	1	2	3	4	5	6	7

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

This command is supported on Catalyst 6500 series switches that are configured with the following modules only:

- WS-X6704-10GE
- WS-X6724-SFP
- WS-X6748-GE-TX

CoS mutation is not supported on non-802.1Q tunnel ports.

When you enter the **mls qos map cos-mutation** command, you are configuring the mutated-CoS values map to sequential ingress-CoS numbers. For example, by entering the **mls qos map cos-mutation 2 3 4 5 6 7 0 1** command, you configure this map:

CoS-in	0	1	2	3	4	5	6	7
CoS-out	2	3	4	5	6	7	0	1

Separate the eight CoS values by a space.

After you define the map in global configuration mode, you can attach the map to a port.

If QoS is disabled, the port is not in a trust CoS mode, and the port is not in 802.1Q tunneling mode. The changes appear once you put the port into trust CoS mode and the port is configured as an 802.1Q tunnel port.

Support for ingress-CoS mutation on 802.1Q tunnel ports and is on a per-port group basis only.

To avoid ingress-CoS mutation configuration failures, only create EtherChannels where all member ports support ingress-CoS mutation or where no member ports support ingress-CoS mutation. Do not create EtherChannels with mixed support for ingress-CoS mutation.

If you configure ingress-CoS mutation on a port that is a member of an EtherChannel, the ingress-CoS mutation is applied to the port-channel interface.

You can configure ingress-CoS mutation on port-channel interfaces.

Examples

This example shows how to define a CoS-to-CoS map:

```
Router(config)# mls qos map cos-mutation test-map 5 4 3 to 1
Router(config)#
```

Related Commands

Command	Description
show mls qos maps	Displays information about the QoS map configuration and run-time version.

mls qos map dscp-cos

To define an egress DSCP-to-CoS map, use the **mls qos map dscp-cos** command. To remove a prior entry, use the **no** form of this command.

mls qos map dscp-cos *dscp-values* **to** *cos-values*

no mls qos map dscp-cos

Syntax Description

dscp-values	DSCP values; valid values are from 0 to 63.
to	Defines mapping.
cos-values	CoS values; valid values are from 0 to 63.

Command Modes

The default DSCP-to-CoS map is listed in Table 2-18.

Table 2-18 DSCP-to-CoS Default Map

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

The DSCP-to-CoS map is used to map the final DSCP classification to a final CoS. This final map determines the output queue and threshold to which the packet is assigned. The CoS map is written into the ISL header or 802.1Q tag of the transmitted packet on trunk interfaces and contains a table of 64 DSCP values and the corresponding CoS values. The Catalyst 6500 series switch has one map.

You can enter up to eight DSCP values separated by a space. You can enter up to eight CoS values separated by a space.

Examples

This example shows how to configure the egress DSCP-to-CoS map for trusted interfaces:

```
Router(config)# mls qos map dscp-cos 20 25 to 3
Router(config)#
```

Related Commands

Command	Description
mls qos map cos-dscp	Defines the ingress CoS-to-DSCP map for trusted interfaces.
show mls qos maps	Displays information about the QoS map configuration and run-time version.

mls qos map dscp-exp

To define the final DSCP classification to the final EXP value, use the **mls qos map dscp-exp** command. To remove a prior entry, use the **no** form of this command.

mls qos map dscp-exp *dscp-values* **to** *exp-values*

no mls qos map dscp-exp

Syntax Description

dscp-values	DSCP values; valid values are from 0 to 63.
to	Defines mapping.
exp-values	EXP values; valid values are from 0 to 7.

Command Modes

The default DSCP-to-EXP map is listed in Table 2-19.

Table 2-19 DSCP-to-EXP Default Map

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
EXP	0	1	2	3	4	5	6	7

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

The DSCP-to-EXP map is used to map the final DSCP classification to a final EXP. This final map determines the output queue and threshold to which the packet is assigned. The EXP map contains a table of 64 DSCP values and the corresponding EXP values. The Catalyst 6500 series switch has one map.

You can enter up to eight DSCP values separated by a space. You can enter up to eight EXP values separated by a space.

Examples

This example shows how to configure the final DSCP classification to a final EXP value:

```
Router(config)# mls qos map dscp-exp 20 25 to 3
Router(config)#
```

Related Commands

Command	Description
show mls qos maps	Displays information about the QoS map configuration and run-time version.

mls qos map dscp-mutation

To define a named DSCP mutation map, use the **mls qos map dscp-mutation** command. To return to the default mapping, use the **no** form of this command.

mls qos map dscp-mutation *map-name input-dscp1* [*input-dscp2* [*input-dscp3* [*input-dscp4* [*input-dscp5* [*input-dscp6* [*input-dscp7* [*input-dscp8*]]]]]]] **to** *output-dscp*

no mls qos map dscp-mutation *map-name*

Syntax Description

map-name	Name of the DSCP mutation map.
input-dscp#	Internal DSCP value; valid values are from 0 to 63. See the "Usage Guidelines" section for additional information.
to	Defines mapping.
output-dscp	Egress DSCP value; valid values are from 0 to 63.

Command Default

output-dscp equals *input-dscp*.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When configuring a named DSCP mutation map, note the following:

- You can enter up to eight input DSCP values that map to a mutated DSCP value.
- You can enter multiple commands to map additional DSCP values to a mutated DSCP value.
- You can enter a separate command for each mutated DSCP value.

You can configure 15 egress-DSCP mutation maps to mutate the internal DSCP value before it is written as the egress-DSCP value. You can attach egress-DSCP mutation maps to any interface that PFC QoS supports.

PFC QoS derives the egress-CoS value from the internal DSCP value. If you configure egress-DSCP mutation, PFC QoS does not derive the egress-CoS value from the mutated DSCP value.

Examples

This example shows how to map DSCP 30 to mutated DSCP value 8:

```
Router(config)# mls qos map dscp-mutation mutemap1 30 to 8
Router(config)#
```

Related Commands

Command	Description
show mls qos maps	Displays information about the QoS map configuration and run-time version.

mls qos map exp-dscp

To define the ingress EXP value to the internal DSCP map, use the **mls qos map exp-dscp** command. To return to the default mappings, use the **no** form of this command.

mls qos map exp-dscp *dscp-values*

no mls qos map exp-dscp

Syntax Description

dscp-values	Interval DSCP values; valid values are from 0 to 63.

Command Default

The default EXP-to-DSCP map is listed in Table 2-20.

Table 2-20 EXP-to-DSCP Default Map

EXP	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The DSCP in these maps refers to the internal DSCP, not the packet DSCP.

The EXP-to-DSCP map is used to map the received EXP value to the internal DSCP map. This final map determines the output queue and threshold to which the packet is assigned. The EXP map contains a table of 64 DSCP values and the corresponding EXP values. The Catalyst 6500 series switch has one map.

You can enter up to eight DSCP values separated by a space.

Examples

This example shows how to configure the received EXP value to an internal DSCP value:

```
Router(config)# mls qos map exp-dscp 20 25 30 31 32 32 33 34
Router(config)#
```

Related Commands

Command	Description
mls qos map exp-mutation	Maps a packet's EXP to a new EXP value.
show mls qos mpls	Displays an interface summary for MPLS QoS classes in the policy maps.

mls qos map exp-mutation

To map a packet's EXP to a new EXP value, use the **mls qos map exp-mutation** command. To return to the default mappings, use the **no** form of this command.

mls qos map exp-mutation *map-name mutated-exp1 mutated-exp2 mutated-exp3 mutated-exp4 mutated-exp5 mutated-exp6 mutated-exp7 mutated-exp8*

no mls qos map exp-mutation *map-name*

Syntax Description

map-name	Name of the EXP-mutation map.
mutated-exp#	Eight EXP values, separated by spaces; valid values are from 0 to 7. See the "Usage Guidelines" section for additional information.

Command Default

If the EXP-to-EXP mutation map is not configured, the default EXP-to-EXP mutation mapping is listed in Table 2-21.

Table 2-21 EXP-to-EXP Mutation Default Map

EXP-in	0	1	2	3	4	5	6	7
EXP-out	0	1	2	3	4	5	6	7

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When you enter the **mls qos map exp-mutation** command, you are configuring the mutated-EXP values map to the sequential EXP numbers. For example, by entering the **mls qos map exp-mutation 2 3 4 5 6 7 0 1** command, you configure this map:

EXP-in	0	1	2	3	4	5	6	7
EXP-out	2	3	4	5	6	7	0	1

Separate the eight EXP values by a space.

After you define the map in global configuration mode, you can attach the map to a port.

You can configure 15 ingress-EXP mutation maps to mutate the internal EXP value before it is written as the ingress-EXP value. You can attach ingress-EXP mutation maps to any interface that PFC QoS supports.

The PFC QoS derives the egress EXP value from the internal DSCP value. If you configure ingress-EXP mutation, PFC QoS does not derive the ingress-EXP value from the mutated EXP value.

Examples

This example shows how to map a packet's EXP to a new EXP value:

```
Router(config)# mls qos map exp-mutation mutemap1 1 2 3 4 5 6 7 0
Router(config)#
```

Related Commands

Command	Description
mls qos map exp-dscp	Defines the ingress EXP value to the internal DSCP map.
show mls qos mpls	Displays an interface summary for MPLS QoS classes in the policy maps.

mls qos map ip-prec-dscp

To define an ingress-IP precedence-to-DSCP map for trusted interfaces, use the **mls qos map ip-prec-dscp** command. To remove a prior entry, use the **no** form of this command.

mls qos map ip-prec-dscp *dscp-values*

no mls qos map ip-prec-dscp

Syntax Description

dscp-values	DSCP values corresponding to IP precedence values 0 to 7; valid values are from 0 to 63.

Command Default

The default IP precedence-to-DSCP configuration is listed in Table 2-22.

Table 2-22 IP Precedence-to-DSCP Default Map

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to map the IP precedence of IP packets arriving on trusted interfaces (or flows) to a DSCP when the trust type is trust-ipprec.

You can enter up to eight DSCP values separated by a space.

This map is a table of eight precedence values (0 through 7) and their corresponding DSCP values. The Catalyst 6500 series switch has one map. The IP precedence values are as follows:

- network **7**
- internet **6**
- critical **5**
- flash-override **4**
- flash **3**
- immediate **2**
- priority **1**
- routine **0**

Examples

This example shows how to configure the ingress-IP precedence-to-DSCP mapping for trusted interfaces:

```
Router(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Router(config)#
```

Related Commands

Command	Description
mls qos map cos-dscp	Defines the ingress CoS-to-DSCP map for trusted interfaces.
mls qos map dscp-cos	Defines an egress DSCP-to-CoS map.
mls qos map policed-dscp	Sets the mapping of policed DSCP values to marked-down DSCP values.
show mls qos maps	Displays information about the QoS map configuration and run-time version.

mls qos map policed-dscp

To configure the DSCP markdown map, use the **mls qos map policed-dscp** command. To remove a prior entry, use the **no** form of this command.

mls qos map policed-dscp {**normal-burst | max-burst**} *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *policed-dscp*

no mls qos map policed-dscp

Syntax Description

normal-burst	Configures the markdown map used by the **exceed-action policed-dscp-transmit** keywords.
max-burst	Configures the markdown map used by the **violate-action policed-dscp-transmit** keywords.
dscp1	DSCP value; valid values are from 0 to 63.
dscp2 through *dscp8*	(Optional) DSCP values; valid values are from 0 to 63.
to	Defines mapping.
policed-dscp	Policed-to-DSCP values; valid values are from 0 to 63.

Command Default

No marked-down values are configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The DSCP-to-policed-DSCP map determines the marked-down DSCP value that is applied to out-of-profile flows. The Catalyst 6500 series switch has one map.

You can enter up to eight DSCP values separated by a space.

You can enter up to eight policed DSCP values separated by a space.

Note To avoid out-of-sequence packets, configure the DSCP-to-policed-DSCP map so that marked-down packets remain in the same queue as the in-profile traffic.

Examples

This example shows how to map multiple DSCPs to a single policed-DSCP value:

```
Router(config)# mls qos map policed-dscp normal-burst 20 25 43 to 4
Router(config)#
```

Related Commands

Command	Description
mls qos map cos-dscp	Defines the ingress CoS-to-DSCP map for trusted interfaces.
mls qos map dscp-cos	Defines an egress DSCP-to-CoS map.
mls qos map ip-prec-dscp	Defines an ingress-IP precedence-to-DSCP map for trusted interfaces.
show mls qos	Displays MLS QoS information.

mls qos marking ignore port-trust

To mark packets even if the interface is trusted, use the **mls qos marking ignore port-trust** command. To return to the default settings, use the **no** form of this command.

mls qos marking ignore port-trust

no mls qos marking ignore port-trust

Syntax Description

This command has no arguments or keywords.

Command Default

Port trust is enabled.

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

Use the **mls qos marking ignore port-trust** command to mark packets even if the interface is trusted.

Examples

This example shows how to mark packets even if the interface is trusted:

```
Router(config)# mls qos marking ignore port-trust
Router(config)#
```

This example shows how to enable port trust:

```
Router(config)# no mls qos marking ignore port-trust
Router(config)#
```

Related Commands

mls qos trust

mls qos marking statistics

To disable allocation of the policer-traffic class identification with set actions, use the **mls qos marking statistics** command. To return to the default settings, use the **no** form of this command.

mls qos marking statistics

no mls qos marking statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **show policy-map interface** command to display policy-map statistics.

Examples

This example shows how to disable the allocation of the policer-traffic class identification with set actions:

```
Router(config)# mls qos marking statistics
Router(config)#
```

This example shows how to allow the allocation of the policer-traffic class identification with set actions:

```
Router(config)# no mls qos marking statistics
Router(config)#
```

Related Commands

Command	Description
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

mls qos mpls trust exp

To set the trusted state of MPLS packets only, use the **mls qos mpls trust exp** command. To set the trusted state of MPLS packets to untrusted, use the **no** form of this command.

mls qos mpls trust exp

no qos mpls trust exp

Syntax Description

This command has no arguments or keywords.

Command Default

With the trusted state enabled, the defaults are as follows:

- Untrusted—The packets are marked to 0 or by policy.
- trust-cos.

With the trusted state disabled, the defaults are as follows:

- trust-exp—The port/policy trust state is ignored.
- The packets are marked by policy.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can enter the **mls qos mpls trust exp** command to treat MPLS packets as other Layer 2 packets for CoS and egress queueing purposes (for example, to apply port or policy trust). All trusted cases (trust CoS/IP/DSCP) are treated as trust-cos.

Examples

This example shows how to set the trusted state of MPLS packets to trust-cos:

```
Router(config-if)# mls qos mpls trust exp
Router(config-if)#
```

This example shows how to set the trusted state of MPLS packets to untrusted:

```
Router(config-if)# no mls qos mpls trust exp
Router(config-if)#
```

Related Commands

Command	Description
show mls qos mpls	Displays an interface summary for MPLS QoS classes in the policy maps.

mls qos police redirected

To turn on ACL-redirected packet policing, use the **mls qos police redirected** command. To turn off policing of ACL-redirected packets, use the **no** form of this command.

mls qos police redirected

no mls qos police redirected

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

Use the **no mls qos police redirected** command whenever you require NDE accuracy (if you do not require QoS-redirected packets).

Examples

This example shows how to turn on the ACL-redirected packet policing:

```
Router(config)# mls qos police redirected
Router(config)#
```

This example shows how to turn off the ACL-redirected packet policing:

```
Router(config)# no mls qos police redirected
Router(config)#
```

Related Commands

Command	Description
show platform earl-mode	Displays platform information.

mls qos protocol

To define the routing-protocol packet policing, use the **mls qos protocol** command. To return to the default settings, use the **no** form of this command.

mls qos protocol *protocol-name* {**pass-through** | {**police** *rate burst*} | {**precedence** *value* [**police** *rate burst*]}}

no mls qos protocol

Syntax Description

protocol-name	Protocol name; valid values are **arp**, **bgp**, **eigrp**, **igrp**, **isis**, **ldp**, **nd**, **ospf**, and **rip**.
pass-through	Specifies pass-through mode.
police *rate*	Specifies the maximum bits per second to be policed; valid values are from 32000 to 10000000000 bits per second.
burst	Normal burst bytes; valid values are from 1000 to 31250000 bytes.
precedence *value*	Specifies the IP-precedence value of the protocol packets to rewrite; valid values are from 0 to 7.

Command Modes

The defaults are as follows:

- *burst* is 1000 bits per second.
- If QoS is enabled, DSCP is rewritten to zero.
- If QoS is disabled, the port is in a pass-through mode (no marking or policing is applied).

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

If you enter the **precedence** *value* keyword and arguments without entering the **police** *rate burst* keyword and arguments, only the packets from an untrusted port are marked.

You can make the protocol packets avoid the per-interface policy maps by entering the **police** *rate*, **pass-through**, or **precedence** *value* keywords and arguments.

The **mls qos protocol** command allows you to define the routing-protocol packet policing as follows:

- When you specify the **pass-through** mode, the DSCP value does not change and is not policed.
- When you set the **police** *rate*, the DSCP value does not change and is policed.
- When you specify the **precedence** *value*, the DSCP value changes for the packets that come from an untrusted port, the CoS value that is based on DSCP-to-CoS map changes, and the traffic is not policed.

- When you specify the **precedence** *value* and the **police** *rate*, the DSCP value changes, the CoS value that is based on DSCP-to-CoS map changes, and the DSCP value is policed. In this case, the DSCP value changes are based on the trust state of the port; the DSCP value is changed only for the packets that come from an untrusted port.
- If you do not enter a **precedence** *value*, the DSCP value is based on whether or not you have enabled MLS QoS as follows:
  - If you enabled MLS QoS and the port is untrusted, the internal DSCP value is overwritten to zero.
  - If you enabled MLS QoS and the port is trusted, then the incoming DSCP value is maintained.

You can make the protocol packets avoid policing completely if you choose the pass-through mode. If the police mode is chosen, the CIR specified is the rate that is used to police all the specified protocol's packets, both entering or leaving the Catalyst 6500 series switch.

To protect the system by ARP broadcast, you can enter the **mls qos protocol arp police** *bps* command.

Examples

This example shows how to define the routing-protocol packet policing:

```
Router(config)# mls qos protocol arp police 43000
Router(config)#
```

This example shows how to avoid policing completely:

```
Router(config)# mls qos protocol arp pass-through 43000
Router(config)#
```

This example shows how to define the IP-precedence value of the protocol packets to rewrite:

```
Router(config)# mls qos protocol bgp precedence 4
Router(config)#
```

This example shows how to define the IP-precedence value of the protocol packets to rewrite and police the DSCP value:

```
Router(config)# mls qos protocol bgp precedence 4 police 32000
Router(config)#
```

Related Commands

Command	Description
show mls qos protocol	Displays the protocol pass-through information.

mls qos queueing-only

To enable port-queueing mode, use the **mls qos queueing-only** command. To disable the port-queueing mode, use the **no** form of this command.

mls qos queueing-only

no mls qos queueing-only

Syntax Description

This command has no arguments or keywords.

Command Default

QoS is globally disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

In port-queueing mode, PFC QoS (marking and policing) is disabled, and packet ToS and CoS are not changed by the PFC. All queueing on rcv and xmt is based on a QoS tag in the incoming packet, which is based on the incoming CoS.

For 802.1Q or ISL-encapsulated port links, queueing is based on the packet 802.1Q or ISL CoS.

For router main interfaces or access ports, queueing is based on the configured per-port CoS (the default CoS is 0).

Examples

This example shows how to enable the port-queueing mode globally:

```
Router(config)# mls qos queueing-only
Router(config)#
```

This example shows how to disable the port-queueing mode globally:

```
Router(config)# no mls qos queueing-only
Router(config)#
```

Related Commands

Command	Description
mls qos (global configuration mode)	Enables the QoS functionality globally.
show mls qos	Displays MLS QoS information.

mls qos queue-mode mode-dscp

To set the queueing mode to DSCP on an interface, use the **mls qos queue-mode mode-dscp** command. To return to the default settings, use the **no** form of this command.

mls qos queue-mode mode-dscp

no mls qos queue-mode mode-dscp

Syntax Description

This command has no arguments or keywords.

Command Default

CoS mode.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is supported on 10-Gigabit Ethernet ports only.

You should configure ports to trust DSCP only if they receive traffic that carries valid Layer 3 DSCP.

You can enable DSCP-based ingress queues and thresholds on WS-X6708-10GE ports to provide congestion avoidance.

For traffic from trust DSCP ports, PFC QoS uses the received DSCP value as the initial internal DSCP value. PFC QoS does not mark any traffic on ingress ports configured to trust received DSCP.

Examples

This example shows how to set the queueing mode to DSCP on an interface:

```
Router(config-if)# mls qos queue-mode mode-dscp
Router(config-if)#
```

Related Commands

Command	Description
priority-queue queue-limit	Allocates the available buffer space to a queue.
show mls qos	Displays MLS QoS information.

mls qos rewrite ip dscp

To enable ToS-to-DSCP rewrite, use the **mls qos rewrite ip dscp** command. To disable ToS-to-DSCP rewrite, use the **no** form of this command.

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

Syntax Description

This command has no arguments or keywords.

Command Default

QoS is globally disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you disable ToS-to-DSCP rewrite, and QoS is enabled globally, the following occurs:

- Final ToS-to-DSCP rewrite is disabled, and the ToS-to-DSCP packet is preserved.
- Policing and marking function according to the QoS configuration.
- Marked and marked-down CoS is used for queueing.
- In QoS disabled mode, both ToS and CoS are preserved.

The **no mls qos rewrite ip dscp** command is incompatible with MPLS. The default **mls qos rewrite ip dscp** command must remain enabled in order for the PFC3BXL or PFC3B to assign the correct EXP value for the labels that it imposes.

Examples

This example shows how to disable ToS-to-DSCP rewrite:

```
Router(config)# mls qos rewrite ip dscp
Router(config)#
```

This example shows how to disable port-queueing mode globally:

```
Router(config)# no mls qos rewrite ip dscp
Router(config)#
```

Related Commands

Command	Description
mls qos (global configuration mode)	Enables the QoS functionality globally.
show mls qos	Displays MLS QoS information.

mls qos statistics-export (global configuration mode)

To enable QoS-statistics data export globally, use the **mls qos statistics-export** command. To disable QoS-statistics data export globally, use the **no** form of this command.

mls qos statistics-export

no mls qos statistics-export

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

You must enable data export globally to set up data export on your Catalyst 6500 series switch.

QoS-statistics data export is not supported on OSM interfaces.

For QoS-statistics data export to perform correctly, you should set the export-destination hostname or IP address and the UDP port number.

Examples

This example shows how to enable data export globally:

```
Router(config)# mls qos statistics-export
Router(config)#
```

This example shows how to disable data export globally:

```
Router(config)# no mls qos statistics-export
Router(config)#
```

Related Commands

Command	Description
show mls qos statistics-export info	Displays information about the MLS-statistics data-export status and configuration.

mls qos statistics-export (interface configuration mode)

To enable per-port QoS-statistics data export, use the **mls qos statistics-export** command. To disable per-port QoS-statistics data export, use the **no** form of this command.

mls qos statistics-export

no mls qos statistics-export

Syntax Description

This command has no arguments or keywords.

Command Modes

Disabled

Command Default

Interface configuration

Command History

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

Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

You must enable data export on the port and globally to set up data export on your Catalyst 6500 series switch.

For QoS-statistics data export to perform correctly, you should set the export-destination hostname or IP address and the UDP port number.

QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the **mls qos statistics-export delimiter** command.

Port statistics are exported; port QoS statistics are not exported. For each data export-enabled port, the following information is exported:

- Type (1 denotes the type of port)
- Module/port
- In packets (cumulated hardware-counter values)
- In bytes (cumulated hardware-counter values)
- Out packets (cumulated hardware-counter values)
- Out bytes (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

For example, if you have QoS-statistics data export that is enabled on FastEthernet4/5, the exported records could be (in this example, the delimiter is a | [pipe]) as follows:

```
|1|4/5|123|80|12500|6800|982361894|
```

Examples

This example shows how to enable QoS-statistics data export:

```
Router(config-if)# mls qos statistics-export
Router(config-if)#
```

This example shows how to disable QoS-statistics data export:

```
Router(config-if)# no mls qos statistics-export
Router(config-if)#
```

Related Commands

Command	Description
mls qos statistics-export delimiter	Sets the QoS-statistics data-export field delimiter.
show mls qos statistics-export info	Displays information about the MLS-statistics data-export status and configuration.

mls qos statistics-export aggregate-policer

To enable QoS-statistics data export on the named aggregate policer, use the **mls qos statistics-export aggregate-policer** command. To disable QoS-statistics data export on the named aggregate policer, use the **no** form of this command.

mls qos statistics-export aggregate-policer *policer-name*

no mls qos statistics-export aggregate-policer *policer-name*

Syntax Description

policer-name	Name of the policer.

Command Modes

Disabled for all shared aggregate policers

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

You must enable data export on the shared aggregate policer and globally to set up data export on your Catalyst 6500 series switch.

QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the **mls qos statistics-export delimiter** command.

For each data export-enabled shared aggregate or named policer, statistics data per policer per EARL is exported. For each data export-enabled shared aggregate or named policer, the following information is exported:

- Type (3 denotes aggregate policer export type)
- Aggregate name
- Direction (in or out)
- EARL identification
- Accepted packets (cumulated hardware-counter values)
- Exceeded normal-rate packets (cumulated hardware-counter values)
- Exceeded excess-rate packets (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

If a shared aggregate policer is attached to policies in both directions, two records are exported (one in each direction). Each record will contain the same counter values for accepted packets, exceeded normal packet rates, and exceeded excess packet rates.

For example, the exported records could be as follows (in this example, the delimiter is a | [pipe]):

```
|3|agg_1|in|1|45543|2345|982361894|
|3|agg_1|in|3|45543|2345|982361894|
```

This example indicates the following information:

- QoS-statistics data export that is enabled on the shared aggregate policer named “aggr_1”
- An EARL in the supervisor engine that is installed in slot 1
- An EARL that is installed in slot 3

Examples

This example shows how to enable per-shared aggregate or named-policer data export:

```
Router(config)# mls qos statistics-export aggregate-policer aggr1M
Router(config)#
```

Related Commands

Command	Description
mls qos statistics-export delimiter	Sets the QoS-statistics data-export field delimiter.
show mls qos statistics-export info	Displays information about the MLS-statistics data-export status and configuration.

mls qos statistics-export class-map

To enable QoS-statistics data export for a class map, use the **mls qos statistics-export class-map** command. To disable QoS-statistics data export for a class map, use the **no** form of this command.

mls qos statistics-export class-map *classmap-name*

no mls qos statistics-export class-map *classmap-name*

Syntax Description

classmap-name	Name of the class map.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

You must enable data export on the class map and globally to set up data export on your Catalyst 6500 series switch.

QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the **mls qos statistics-export delimiter** command.

For each data export-enabled class map, the statistics data per policer per interface is exported. If the interface is a physical interface, the following information is exported:

- Type (4 denotes a class map physical export)
- Class map name
- Direction (in or out)
- Module/port
- Accepted packets (cumulated hardware-counter values)
- Exceeded normal-rate packets (cumulated hardware-counter values)
- Exceeded excess-rate packets (cumulated hardware-ounter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

If the interface is a Catalyst 6500 series switch VLAN, the following information is exported:

- Type (5 denotes class-map VLAN export)
- Class-map name
- Direction (in or out)
- EARL identification (slot number in which the EARL is installed)

- VLAN number
- Accepted packets (cumulated hardware-counter values)
- Exceeded normal-rate packets (cumulated hardware-counter values)
- Exceeded excess-rate packets (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

If the interface is a Catalyst 6500 series switch port channel, the following information is exported:

- Type (6 denotes class-map port-channel export)
- Class-map name
- Direction (in or out)
- EARL identification (slot number in which the EARL is installed)
- Port-channel number
- Accepted packets (cumulated hardware-counter values)
- Exceeded normal-rate packets (cumulated hardware-counter values)
- Exceeded excess-rate packets (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

For example, if you have the following configuration:

- QoS-statistics data export enabled on the class map named “class_1”
- An EARL in the supervisor engine that is installed in slot 1
- An EARL that is installed in slot 3
- The Catalyst 6500 series switch is in the policy map named “policy_1”
- policy_1 is attached to the following interfaces in the ingress direction:
  - FastEthernet4/5
  - VLAN 100
  - Port-channel 24

The exported records could be (in this example, the delimiter is a | [pipe]) as follows:

```
|4|class_1|in|4/5|45543|2345|2345|982361894|
|5|class_1|in|1|100|44000|3554|36678|982361894|
|5|class_1|in|3|100|30234|1575|1575|982361894|
```

Examples

This example shows how to enable QoS-statistics data export for a class map:

```
Router(config)# mls qos statistics-export class-map class3
Router(config)#
```

Related Commands

Command	Description
mls qos statistics-export delimiter	Sets the QoS-statistics data-export field delimiter.
show mls qos statistics-export info	Displays information about the MLS-statistics data-export status and configuration.

mls qos statistics-export delimiter

To set the QoS-statistics data-export field delimiter, use the **mls qos statistics-export delimiter** command. To return to the default settings, use the **no** form of this command.

mls qos statistics-export delimiter

no mls qos statistics-export delimiter

Syntax Description

This command has no arguments or keywords.

Command Default

The default delimiter is the pipe character (|).

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

You must enable data export globally to set up data export on your Catalyst 6500 series switch.

Examples

This example shows how to set the QoS-statistics data-export field delimiter (a comma) and verify the configuration:

```
Router(config)# mls qos statistics-export delimiter ,
Router(config)#
```

Related Commands

Command	Description
show mls qos statistics-export info	Displays information about the MLS-statistics data-export status and configuration.

mls qos statistics-export destination

To configure the QoS-statistics data-export destination host and UDP port number, use the **mls qos statistics-export destination** command. To return to the default settings, use the **no** form of this command.

mls qos statistics-export destination {*host-name* | *host-ip-address*} {{**port** *port-number*} | **syslog**} [**facility** *facility-name*] [**severity** *severity-value*]

Syntax Description

host-name	Hostname.
host-ip-address	Host IP address.
port *port-number*	Specifies the UDP port number.
syslog	Specifies the syslog port.
facility *facility-name*	(Optional) Specifies the type of facility to export; see the "Usage Guidelines" section for a list of valid values.
severity *severity-value*	(Optional) Specifies the severity level to export; see the "Usage Guidelines" section for a list of valid values.

Command Default

The default is none unless **syslog** is specified. If **syslog** is specified, the defaults are as follows:

- *port* is **514**.
- *facility* is **local6**.
- *severity* is **debug**.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

Valid *facility* values are as follows:

- **authorization**—Security/authorization messages
- **cron**—Clock daemon
- **daemon**—System daemon
- **kernel**—Kernel messages
- **local0**—Local use 0
- **local1**—Local use 1
- **local2**—Local use 2

- **local3**—Local use 3
- **local4**—Local use 4
- **local5**—Local use 5
- **local6**—Local use 6
- **local7**—Local use 7
- **lpr**—Line printer subsystem
- **mail**—Mail system
- **news**—Network news subsystem
- **syslog**—Messages that are generated internally by syslogd
- **user**—User-level messages
- **uucp**—UUCP subsystem

Valid *severity* levels are as follows:

- **alert**—Action must be taken immediately
- **critical**—Critical conditions
- **debug**—Debug-level messages
- **emergency**—System is unusable
- **error**—Error conditions
- **informational**—Informational
- **notice**—Normal but significant conditions
- **warning**—Warning conditions

Examples

This example shows how to specify the destination host address and syslog as the UDP port number:

```
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
Router(config)#
```

Related Commands

Command	Description
show mls qos statistics-export info	Displays information about the MLS-statistics data-export status and configuration.

mls qos statistics-export interval

To specify how often a port and/or aggregate-policer QoS-statistics data is read and exported, use the **mls qos statistics-export interval** command. To return to the default settings, use the **no** form of this command.

mls qos statistics-export interval *interval*

no mls qos statistics-export interval

Syntax Description

interval	Export time; valid values are from 30 to 65535 seconds.

Command Default

300 seconds

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

The *interval* needs to be short enough to avoid counter wraparound with the activity in your configuration.

Caution Be careful when decreasing the interval because exporting QoS statistics increases the traffic on the Catalyst 6500 series switch.

Examples

This example shows how to set the QoS-statistics data-export interval:

```
Router(config)# mls qos statistics-export interval 250
Router(config)#
```

Related Commands

Command	Description
show mls qos statistics-export info	Displays information about the MLS-statistics data-export status and configuration.

mls qos trust

To set the trusted state of an interface, use the **mls qos trust** command. To set an interface to the untrusted state, use the **no** form of this command.

mls qos trust [**cos** | **dscp** | **ip-precedence**]

no mls qos trust

Syntax Description

cos	(Optional) Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
dscp	(Optional) Specifies that the ToS bits in the incoming packets contain a DSCP value.
ip-precedence	(Optional) Specifies that the ToS bits in the incoming packets contain an IP precedence value and derives the internal DSCP value from the IP-precedence bits.

Command Default

The defaults for LAN interfaces and WAN interfaces on the OSMs are as follows:

- If you enable global QoS, the port is untrusted.
- If you disable global QoS, the default is **dscp**.
- If you do not enter an argument, **trust dscp** is assumed.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can enter the **mls qos trust** command to set the trusted state of an interface. For example, you can set whether the packets arriving at an interface are trusted to carry the correct CoS, ToS, and DSCP classifications.

The **cos** keyword is not supported for **pos** or **atm** interface types.

You cannot configure the trust state on FlexWAN modules.

You cannot configure the trust state on 1q4t LAN ports except for Gigabit Ethernet ports.

Ingress-queue drop thresholds are not implemented when you enter the **mls qos trust cos** command on 4-port Gigabit Ethernet WAN modules.

Use the **set qos-group** command to set the trust state on Layer 2 WAN interfaces.

Examples

This example shows how to set the trusted state of an interface to IP precedence:

```
Router(config-if)# mls qos trust ip-precedence
Router(config-if)#
```

Related Commands

Command	Description
mls qos bridged	Enables the microflow policing for bridged traffic on Layer 3 LAN interfaces.
mls qos cos	Defines the default CoS value for an interface.
mls qos vlan-based	Defines the default CoS value for a VLAN.
show queueing interface	Displays queueing information.

mls qos trust extend

To configure the trust mode of the phone, use the **mls qos trust extend** command. To return to the default settings, use the **no** form of this command.

mls qos trust extend [**cos** *value*]

no mls qos trust extend

Syntax Description

cos *value*	(Optional) Specifies the CoS value that is used to remark the packets from the PC; valid values are from 0 to 7.

Command Default

The default settings are as follows:

- Mode is untrusted.
- **cos** *value* is 0.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is not supported on WAN modules.

If you set the phone to trusted mode, all the packets from the PC are sent untouched directly through the phone to the Catalyst 6500 series switch. If you set the phone to untrusted mode, all the traffic coming from the PC are remarked with the configured CoS value before being sent to the Catalyst 6500 series switch.

Each time that you enter the **mls qos trust extend** command, the mode is changed. For example, if the mode was previously set to trusted, if you enter the command, the mode changes to untrusted. Enter the **show queueing interface** command to display the current trust mode.

Examples

This example shows how to set the phone that is attached to the switch port in trust mode:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend
Router(config-if)#
```

This example shows how to change the mode to untrusted and set the remark CoS value to 3:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend cos 3
Router(config-if)#
```

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

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no mls qos trust extend
Router(config-if)#
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

mls qos vlan-based

To enable per-VLAN QoS for a Layer 2 interface, use the **mls qos vlan-based** command. To disable per-VLAN QoS for a Layer 2 interface, use the **no** form of this command.

mls qos vlan-based

no mls qos vlan-based

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

In VLAN-based mode, the policy map that is attached to the Layer 2 interface is ignored, and QoS is driven by the policy map that is attached to the corresponding VLAN interface.

You can configure per-VLAN QoS only on Layer 2 interfaces.

Note Layer 3 interfaces are always in interface-based mode. Layer 3 VLAN interfaces are always in VLAN-based mode.

Examples

This example shows how to enable per-VLAN QoS for a Layer 2 interface:

```
Router(config-if)# mls qos vlan-based
Router(config-if)#
```

Related Commands

Command	Description
mls qos bridged	Enables the microflow policing for bridged traffic on Layer 3 LAN interfaces.
mls qos cos	Defines the default CoS value for an interface.
show queueing interface	Displays queueing information.

mls rate-limit all

To enable and set the rate limiters common to unicast and multicast packets, use the **mls rate-limit all** command. To disable the rate limiters, use the **no** form of this command.

mls rate-limit all {**mtu-failure** | **ttl-failure**} *pps* [*packets-in-burst*]

no mls rate-limit all {**mtu-failure** | **ttl-failure**}

Syntax Description

all	Specifies rate limiting for unicast and multicast packets.
mtu-failure	Enables and sets the rate limiters for MTU-failed packets.
ttl-failure	Enables and sets the rate limiters for TTL-failed packets.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The Layer 2 rate limiters are off by default. If you enable and set the rate limiters, the default *packets-in-burst* is **10**.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Rate limiters can rate limit packets that are punted from the data path in the hardware up to the data path in the software. Rate limiters protect the control path in the software from congestion by dropping the traffic that exceeds the configured rate.

Examples

This example shows how to set the TTL-failure limiter for unicast and multicast packets:

```
Router(config)# mls rate-limit all ttl-failure 15
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit layer2

To enable and rate limit the control packets in Layer 2, use the **mls rate-limit layer2** command. To disable the rate limiter in the hardware, use the **no** form of this command.

mls rate-limit layer2 {**pdu** | **l2pt** | **port-security**} *pps* [*packets-in-burst*]

no mls rate-limit layer2 [**pdu** | **l2pt** | **port-security**]

Syntax Description

pdu *pps*	Specifies the rate limit for BPDU, CDP, PDU, and VTP PDU Layer 2 control packets; valid values are from 10 to 1000000 packets per second.
l2pt *pps*	Specifies the rate limit for control packets in Layer 2 with a protocol-tunneling multicast-MAC address in Layer 2; valid values are from 10 to 1000000 packets per second.
port-security *pps*	Specifies the rate limit for port security traffic; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The default settings are as follows:

- Layer 2 rate limiters are off by default.
- If you enable and set the rate limiters, the default setting for *packets-in-burst* is **10** and *pps* has no default setting.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

You cannot configure the Layer 2 rate limiters if the global switching mode is set to truncated mode.

For the **port-security** *pps* keywords and argument, use the following guidelines:

- The PFC2 does not support the port-security rate limiter.
- The truncated switching mode does not support the port-security rate limiter.
- The lower the value, the more the CPU is protected.

Rate limiters control packets as follows:

- The frames are classified as Layer 2 control frames by the destination MAC address. The destination MAC address used are as follows:
  - 0180.C200.0000 for IEEE BPDU
  - 0100.0CCC.CCCC for CDP
  - 0100.0CCC.CCCD for PVST/SSTP BPDU

- The software allocates an LTL index for the frames.
- The LTL index is submitted to the forwarding engine for aggregate rate limiting of all the associated frames.

The Layer 2 control packets are as follows:

- GVRP
- BPDUs
- CDP/DTP/PAgP/UDLD/LACP/VTP PDUs
- PVST/SSTP PDUs

If the rate of the traffic exceeds the configured *rate*, the excessive packets are dropped at the hardware.

The **pdu** and **l2pt** rate limiters use specific hardware rate-limiter numbers only, such as 9 through 12. Enter the **show mls rate-limit usage** command to display the available rate-limiter numbers. The available numbers are displayed as "Free" in the output field. If all four rate limiters are in use by other features, a system message is displayed telling you to turn off a feature to rate limit the control packets in Layer 2.

When a MAC move occurs and a packet is seen on two ports, the packet is redirected to the software. If one of those ports has the violation mode set to restrict or protect, the packet is dropped in software. You can use the port-security rate limiter to throttle the amount of such packets redirected to software . This helps in protecting the software from high traffic rates.

Examples

This example shows how to enable and set the rate limiters for the protocol-tunneling packets in Layer 2:

```
Router(config)# mls rate-limit layer2 l2pt 3000
Router(config)#
```

This example shows how to configure the port-security rate limiter:

```
Router(config)# mls rate-limit layer2 port-security 500
Router(config)# end
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit multicast ipv4

To enable and set the rate limiters for the IPv4 multicast packets, use the **mls rate-limit multicast ipv4** command. To disable the rate limiters, use the **no** form of this command.

mls rate-limit multicast ipv4 {**connected** | **fib-miss** | **igmp** | **ip-option** | **partial** | **non-rpf**} *pps* [*packets-in-burst*]

no mls rate-limit multicast ipv4 {**connected** | **fib-miss** | **igmp** | **ip-option** | **partial** | **non-rpf**}

Syntax Description

connected	Enables and sets the rate limiters for multicast packets from directly connected sources.
fib-miss	Enables and sets the rate limiters for the FIB-missed multicast packets.
igmp	Enables and sets the rate limiters for the IGMP packets.
ip-option	Enables and sets the rate limiters for the multicast packets with IP options.
partial	Enables and sets the rate limiters for the multicast packets during a partial SC state.
non-rpf	Enables and sets the rate limiters for the multicast packets failing the RPF check.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **100** is programmed for multicast cases.
- **fib-miss**—Enabled at **100000** *pps* and *packet-in-burst* is set to **100**.
- **ip-option**—Disabled.
- **partial**—Enabled at **100000** *pps* and *packet-in-burst* is set to **100**.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

You cannot configure the IPv4 rate limiters if the global switching mode is set to truncated mode.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

The **ip-option** keyword is supported in PFC3BXL or PFC3B mode only.

Examples

This example shows how to set the rate limiters for the multicast packets failing the RPF check:

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
Router(config)#
```

This example shows how to set the rate limiters for the multicast packets during a partial SC state:

```
Router(config)# mls rate-limit multicast ipv4 partial 250
Router(config)#
```

This example shows how to set the rate limiters for the FIB-missed multicast packets:

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 15
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit multicast ipv6

To configure the IPv6 multicast rate limiters, use the **mls rate-limit multicast ipv6** command. To disable the rate limiters, use the **no** form of this command.

mls rate-limit multicast ipv6 {**connected** *pps* [*packets-in-burst*]} | {*rate-limiter-name* {**share** {**auto** | *target-rate-limiter*}}}

no mls rate-limit multicast ipv6 {**connected** | *rate-limiter-type*}

Syntax Description

connected *pps*	Enables and sets the rate limiters for the IPv6 multicast packets from a directly connected source; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
rate-limiter-name	Rate-limiter name; valid values are **default-drop**, **route-cntl**, **secondary-drop**, **sg**, **starg-bridge**, and **starg-m-bridge**. See the "Usage Guidelines" section for additional information.
share	Specifies the sharing policy for IPv6 rate limiters; see the "Usage Guidelines" section for additional information.
auto	Decides the sharing policy automatically.
target-rate-limiter	Rate-limiter name that was the first rate-limiter name programmed in the hardware for the group; valid values are **default-drop**, **route-cntl**, **secondary-drop**, **sg**, **starg-bridge**, and **starg-m-bridge**. See the "Usage Guidelines" section for additional information.

Command Default

If the *burst* is not set, a default of **100** is programmed for multicast cases.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The *rate-limiter-name* argument must be a rate limiter that is not currently programmed.

The *target-rate-limiter* argument must be a rate limiter that is programmed in the hardware and must be the first rate limiter programmed for its group.

Table 2-23 lists the IPv6 rate limiters and the class of traffic that each rate limiter serves.

Table 2-23 IPv6 Rate Limiters

Rate-Limiter ID	Traffic Classes to be Rate Limited
Connected	Directly connected source traffic
Default-drop	* (*, G/m)SSM * (*, G/m)SSM non-rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT threshold is infinity
SG	* (S, G) RP-RPF post-switchover * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM * SM non-rpf traffic when (*, G) exists
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * SM non-rpf traffic when (*, G) does not exist

You can configure rate limiters for IPv6 multicast traffic using one of the following methods:

- Direct association of the rate limiters for a traffic class—Select a rate and associate the rate with a rate limiter. This example shows how to pick a rate of 1000 pps and 20 packets per burst and associate the rate with the **default-drop** rate limiter:

  ```
  Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
  ```

- Static sharing of a rate limiter with another preconfigured rate limiter—When there are not enough adjacency-based rate limiters available, you can share a rate limiter with an already configured rate limiter (target rate limiter). This example shows how to share the **route-cntl** rate limiter with the **default-drop** target rate limiter:

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
  ```

  If the target rate limiter is not configured, a message displays that the target rate limiter must be configured for it to be shared with other rate limiters.

- Dynamic sharing of rate limiters—If you are not sure about which rate limiter to share with, use the **share auto** keywords to enable dynamic sharing. When you enable dynamic sharing, the system picks a preconfigured rate limiter and shares the given rate limiter with the preconfigured rate limiter. This example shows how to choose dynamic sharing for the **route-cntrl** rate limiter:

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
  ```

Examples

This example shows how to set the rate limiters for the IPv6 multicast packets from a directly connected source:

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

This example shows shows how to configure a direct association of the rate limiters for a traffic class:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
Router(config)#
```

This example shows how to configure the static sharing of a rate limiter with another preconfigured rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

This example shows how to enable dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast acl

To enable and set the ACL-bridged rate limiters, use the **mls rate-limit unicast acl** command. To disable the rate limiters, use the **no** form of this command.

mls rate-limit unicast acl {**input** | **output** | **vacl-log**} {*pps* [*packets-in-burst*]}

no mls rate-limit unicast acl {**input** | **output** | **vacl-log**}

Syntax Description

input	Specifies the rate limiters for the input ACL-bridged unicast packets.
output	Specifies the rate limiters for the output ACL-bridged unicast packets.
vacl-log	Specifies the rate limiters for the VACL log cases.
pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- **input**—Disabled.
- **output**—Disabled.
- **vacl-log**—Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases—10 to 1000000 *pps*
- VACL log cases—10 to 5000 *pps*

You cannot change the **vacl-log** *packets-in-burst* keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets

- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failures use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected if the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the input ACL-bridged packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast acl ingress 100
Router(config)#
```

This example shows how to disable the input ACL-bridged packet limiter for unicast packets:

```
Router(config)# no mls rate-limit unicast acl ingress
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast cef

To enable and set the CEF rate limiters, use the **mls rate-limit unicast cef** command. To disable the rate limiters, use the **no** form of this command.

mls rate-limit unicast cef {**receive** | **glean**} *pps* [*packets-in-burst*]

no mls rate-limit unicast cef {**receive** | **glean**}

Syntax Description

receive	Enables and sets the rate limiters for receive packets.
glean	Enables and sets the rate limiters for ARP-resolution packets.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- **receive**—Disabled.
- **glean**—Disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you enable the CEF rate limiters, the following situations occur (if the situation that is listed is unacceptable, disable the CEF rate limiters):

- If a packet hits a glean/receive adjacency, the packet may be dropped instead of being sent to the software if there is an output ACL on the input VLAN and the matched entry result is deny.
- If the matched ACL entry result is bridge, the packet is subject to egress ACL bridge rate limiting (if turned ON) instead of glean/receive rate limiting.
- The glean/receive adjacency rate limiting is applied only if the output ACL lookup result is permit or there is no output ACLs on the input VLAN.

Examples

This example shows how to set the CEF-glean limiter for the unicast packets:

```
Router(config)# mls rate-limit unicast cef glean 5000
Router(config)#
```

This example shows disable the CEF-glean limiter for the unicast packets:

```
Router(config)# no mls rate-limit unicast cef glean
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast ip

To enable and set the rate limiters for the unicast packets, use the **mls rate-limit unicast ip** command. To disable the rate limiters, use the **no** form of this command.

mls rate-limit unicast ip {**errors** | **features** | **options** | **rpf-failure**} *pps* [*packets-in-burst*]

mls rate-limit unicast ip icmp {**redirect** | **unreachable** {**acl-drop** *pps*} | **no-route** *pps*} [*packets-in-burst*]

no mls rate-limit unicast ip {**errors** | **features** | {**icmp** {**redirect** | **unreachable** {**acl-drop** | **no-route**}}} | **options** | **rpf-failure**} *pps* [*packets-in-burst*]

Syntax Description

errors	Specifies rate limiting for unicast packets with IP checksum and length errors.
features	Specifies rate limiting for unicast packets with software-security features in Layer 3 (for example, authorization proxy, IPsec, and inspection).
options	Specifies rate limiting for unicast IPv4 packets with options.
rpf-failure	Specifies rate limiting for unicast packets with RPF failures.
pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
icmp redirect	Specifies rate limiting for unicast packets requiring ICMP redirect.
icmp unreachable acl-drop *pps*	Enables and sets the rate limiters for the ICMP unreachables for the ACL-dropped packets.
icmp unreachable no-route *pps*	Enables and sets the rate limiters for the ICMP unreachables for the FIB-miss packets.

Command Default

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **10** is programmed as the burst for unicast cases.
- **errors**—Enabled at **100** *pps* and *packets-in-burst* set to **10**.
- **rpf-failure**—Enabled at **100** *pps* and *packets-in-burst* set to **10**.
- **icmp unreachable acl-drop**—Enabled at **100** *pps* and *packets-in-burst* set to **10**.
- **icmp unreachable no-route**—Enabled at **100** *pps* and *packets-in-burst* set to **10**.
- **icmp redirect**—Disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

To provide OAL support for denied packets, enter the **mls rate-limit unicast ip icmp unreachable acl-drop 0** command.

OAL and VACL capture are incompatible. Do not configure both features on the switch. With OAL configured, use SPAN to capture traffic.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

Note When you configure an ICMP rate limiter, and an ICMP redirect occurs, exiting data traffic is dropped while the remaining traffic on the same interface is forwarded.

When setting the *pps*, the valid values are **0** and from 10 to 1000000. Setting the *pps* to **0** globally disables the redirection of the packets to the route processor. The **0** value is supported for these rate limiters:

- ICMP unreachable ACL-drop
- ICMP unreachable no-route
- ICMP redirect
- IP rpf failure

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failures use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the ICMP-redirect limiter for unicast packets:

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast l3-features

To enable and set the Layer 3 security rate limiters for the unicast packets, use the **mls rate-limit unicast l3-features** command. To disable the rate limiters, use the **no** form of this command.

mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

no mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

Syntax Description

pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to set the Layer 3 security rate limiters for the unicast packets:

```
Router(config)# mls rate-limit unicast l3-features 5000
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast vacl-log

To enable and set the VACL-log case rate limiters, use the **mls rate-limit unicast vacl-log** command. To disable the rate limiters, use the **no** form of this command.

mls rate-limit unicast vacl-log {*pps* [*packets-in-burst*]}

no mls rate-limit unicast vacl-log

Syntax Description

pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases—10 to 1000000 *pps*
- VACL log cases—10 to 5000 *pps*

Setting the *pps* to **0** globally disables the redirection of the packets to the route processor.

You cannot change the **vacl-log** *packets-in-burst* keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route

  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failures use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected if the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the VACL-log case packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast vacl-log 100
Router(config)#
```

This example shows how to disable the rate limiters:

```
Router(config)# no mls rate-limit unicast vacl-log 100
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rp ip (global configuration mode)

To enable external systems to establish IP shortcuts to the PISA, use the **mls rp ip** command. To remove a prior entry, use the **no** form of this command.

mls rp ip [**input-acl** | **route-map**]

no mls rp ip

Syntax Description

input-acl	(Optional) Enables the IP-input access list.
route-map	(Optional) Enables the IP-route map.

Command Default

No shortcuts are configured.

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to allow the external systems to establish IP shortcuts with IP-input access lists:

```
Router(config)# mls rp ip input-acl
Router(config)#
```

Related Commands

Command	Description
mls ip	Enables MLS IP for the internal router on the interface.
show mls ip multicast	Displays the MLS IP information.

mls rp ip (interface configuration mode)

To enable the external systems to enable MLS IP on a specified interface, use the **mls rp ip** command. To disable MLS IP, use the **no** form of this command.

mls rp ip

no mls rp ip

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to enable the external systems to enable MLS IP on an interface:

```
Router(config-if)# mls rp ip
Router(config-if)
```

Related Commands

Command	Description
mls rp ip (global configuration mode)	Enables external systems to establish IP shortcuts to the PISA.
show mls ip multicast	Displays the MLS IP information.

mls rp ipx (global configuration mode)

To allow the external systems to enable MLS IPX to the PISA, use the **mls rp ipx** command. To remove a prior entry, use the **no** form of this command.

mls rp ipx [**input-acl**]

no mls rp ipx

Syntax Description

input-acl	(Optional) Enables MLS IPX and overrides ACLs.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to allow the external systems to enable MLS IPX to the PISA and override ACLs:

```
Router(config)# mls rp ipx input-acl
Router(config)#
```

Related Commands

Command	Description
mls rp ipx (interface configuration mode)	Allows the external systems to enable MLS IPX on the interface.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.

mls rp ipx (interface configuration mode)

To allow the external systems to enable MLS IPX on the interface, use the **mls rp ipx** command. To disable MLS IPX on the interface, use the **no** form of this command.

mls rp ipx

no mls rp ipx

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to allow the external systems to enable MLS IPX on an interface:

```
Router(config-if)# mls rp ipx
Router(config-if)#
```

Related Commands

Command	Description
mls rp ipx (global configuration mode)	Allows the external systems to enable MLS IPX to the PISA.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.

mls rp management-interface

To enable the interface as a management interface, use the **mls rp management-interface** command. To remove a prior entry, use the **no** form of this command.

mls rp management-interface

no mls rp management-interface

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to enable an interface as a management interface:

```
Router(config-if)# mls rp management-interface
Router(config-if)#
```

Related Commands

Command	Description
show mls rp	Displays MLS details.

mls rp nde-address

To specify the NDE address, use the **mls rp nde-address** command. To remove a prior entry, use the **no** form of this command.

mls rp nde-address *ip-address*

no mls rp nde-address *ip-address*

Syntax Description

ip-address	NDE IP address.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the following syntax to specify an IP subnet address:

- *ip-subnet-addr*—Short subnet address format. The trailing decimal number 00 in an IP address YY.YY.YY.00 specifies the boundary for an IP-subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip-addr/subnet-mask*—Long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip-addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip-addr/maskbits*—Simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip-addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip-subnet-addr.*

Examples

This example shows how to set the NDE address to 170.25.2.1:

```
Router(config)# mls rp nde-address 170.25.2.1
Router(config)#
```

Related Commands

Command	Description
show mls rp	Displays MLS details.

mls rp vlan-id

To assign a VLAN ID to the interface, use the **mls rp vlan-id** command. To remove a prior entry, use the **no** form of this command.

mls rp vlan-id {*vlan-id*}

no mls rp vlan-id

Syntax Description

vlan-id	VLAN ID number; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to assign a VLAN ID to the interface:

```
Router(config-if)# mls rp vlan-id 4
Router(config-if)#
```

Related Commands

Command	Description
show mls rp	Displays MLS details.

mls rp vtp-domain

To link the interface to a VTP domain, use the **mls rp vtp-domain** command. To remove a prior entry, use the **no** form of this command.

mls rp vtp-domain *name*

no mls rp vtp-domain *name*

Syntax Description

name	VLAN domain name.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to link the interface to a VTP domain:

```
Router(config-if)# mls rp vtp-domain EverQuest
Router(config-if)#
```

Related Commands

Command	Description
show mls rp	Displays MLS details.
vtp	Configures the global VTP state.

mls sampling

To enable the sampled NetFlow and specify the sampling method, use the **mls sampling** command. To disable the sampled NetFlow, use the **no** form of this command.

mls sampling {{**time-based** *rate*} | {**packet-based** *rate* [*interval*]}}

no mls sampling

Syntax Description

time-based *rate*	Specifies the time-based sampling rate; valid values are **64**, **128**, **256**, **512**, **1024**, **2046**, **4096**, and **8192**. See the "Usage Guidelines" section for additional information.
packet-based *rate*	Specifies the packet-based sampling rate; valid values are **64**, **128**, **256**, **512**, **1024**, **2046**, **4096**, and **8192**.
interval	(Optional) Sampling interval; valid values are from 8000 to 16000 milliseconds.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

To enable sampling on the PFC3, you must enter the **mls sampling** command and the **mls netflow sampling** command on the appropriate interfaces. If you do not enter the **mls netflow sampling** command, NDE will not export flows.

The sampled NetFlow is supported on Layer 3 interfaces only.

You can enable the sampled NetFlow even if NDE is disabled, but no flows are exported.

With packet-based sampling, a flow with a packet count of n is sampled n/m times, where m is the sampling rate.

The time-based sampling is based on a preset interval for each sampling rate. Table 2-24 lists the sample intervals for each rate and period.

Table 2-24 Time-Based Sampling Intervals

Sampling Rate	Sampling Time (milliseconds)	Export Interval (Milliseconds)
1 in 64	128	8192
1 in 128	64	8192
1 in 256	32	8192
1 in 512	16	8192

Table 2-24 Time-Based Sampling Intervals (continued)

Sampling Rate	Sampling Time (milliseconds)	Export Interval (Milliseconds)
1 in 1024	8	8192
1 in 2048	4	8192
1 in 4096	4	16384
1 in 8192	4	32768

Examples

This example shows how to enable the time-based NetFlow sampling and set the sampling rate:

```
Router(config)# mls sampling time-based 1024
Router(config)#
```

This example shows how to enable the packet-based NetFlow sampling and set the sampling rate and interval:

```
Router(config)# mls sampling packet-based 1024 8192
Router(config)#
```

Related Commands

Command	Description
mls netflow sampling	Enables the sampled NetFlow on an interface.
show mls sampling	Displays information about the sampled NDE status.

mls switching

To enable the hardware switching, use the **mls switching** command. To disable hardware switching, use the **no** form of this command.

mls switching

no mls switching

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Examples

This example shows how to enable the hardware switching:

```
Router(config)# mls switching
Router(config)#
```

This example shows how to disable the hardware switching:

```
Router(config)# no mls switching
Router(config)#
```

Related Commands

Command	Description
mls switching unicast	Enables the hardware switching of the unicast traffic for an interface.

mls switching unicast

To enable the hardware switching of the unicast traffic for an interface, use the **mls switching unicast** command. To disable the hardware switching of the unicast traffic for an interface, use the **no** form of this command.

mls switching unicast

no mls switching unicast

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to enable the hardware switching for an interface:

```
Router(config-if)# mls switching unicast
Router(config-if)#
```

This example shows how to disable the hardware switching for an interface:

```
Router(config-if)# no mls switching unicast
Router(config-if)#
```

Related Commands

Command	Description
mls switching	Enables hardware switching.

mls verify

To enable hardware packet parsing error checks, use the **mls verify** command. To disable Layer 3 error checking in the hardware, use the **no** form of this command.

mls verify {**ip** | **ipx**} {**checksum** | {**length** {**consistent** | **minimum**}} | **same-address** | **syslog**}

no mls verify {**ip** | **ipx**} {**checksum** | {**length** {**consistent** | **minimum**}} **same-address** | **syslog**}

Syntax Description

ip	Specifies the IP checksum errors.
ipx	Specifies the IPX checksum errors.
checksum	Specifies the checksum-error check.
length consistent	Checks the length in the header against the physical frame length.
length minimum	Checks the minimum packet length.
same-address	Checks for the packets that have equal source and destination IP addresses.
syslog	Specifies the syslog packet parse error traps.

Command Default

The default settings are as follows:

- **checksum**
- **same-address** is disabled.
- **syslog** is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The IP too-short packets are the IP packets with an IP header length or IP total length field that is smaller than 20 bytes.

When you enter the **mls verify ip length minimum** command, valid IPv4 packets are switched in the hardware only if the IP protocol fields are equal to one of the following types:

- ICMP (1)
- IGMP (2)
- IP (4)
- TCP (6)
- UDP (17)
- IPv6 (41)

- GRE (47)
- SIPP-ESP (50)

When you enter the **no mls verify ip length minimum** command, too-short packets are switched in the hardware. The too-short packets that have IP protocol = 6 (TCP) are sent to the software.

To prevent packets with the same source and destination IP address from being switched in the hardware, use the **mls verify ip same-address** command.

Examples

This example shows how to enable Layer 3 error checking in the hardware:

```
Router(config)# mls verify ip checksum
Router(config)#
```

This example shows how to disable Layer 3 error checking in the hardware:

```
Router(config)# no mls verify ip checksum
Router(config)#
```

This example shows how to prevent packets with the same source and destination IP address from being switched in the hardware:

```
Router(config)# mls verify ip same-address
Router(config)#
```

mobility

To configure the wireless mGRE tunnels, use the **mobility** command. To return to the default settings, use the **no** form of this command.

mobility {**network-id** *id*} | {**tcp adjust-mss**}

mobility [**trust** | **broadcast**]

Syntax Description

network-id *id*	Specifies the wireless network ID for the mGRE tunnel; valid values are from 1 to 4095.
tcp adjust-mss	Adjusts the MSS value in TCP SYN and TCP ACK on the access points automatically.
trust	(Optional) Specifies the trusted network.
broadcast	(Optional) Specifies that the mGRE tunnel convert the NBMA to the BMA.

Command Default

Untrusted network

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

The **tcp adjust-mss** keywords are supported on mGRE tunnel interfaces only.

You can enter the **ip tcp adjust-mss** *value* command to change the TCP MSS to a lower value.

A trusted network can use DHCP or a static IP address. An untrusted network supports only DHCP clients.

Examples

This example shows how to specify the network identification number for the mGRE tunnel:

```
Router (config-if)# mobility network-id 200
Router (config-if)#
```

This example shows how to specify the trusted network:

```
Router (config-if)# mobility trust
Router (config-if)#
```

This example shows how to specify that the mGRE tunnel convert the NBMA to the BMA:

```
Router (config-if)# mobility broadcast
Router (config-if)#
```

This example shows how to adjust the MSS value in TCP SYN and TCP ACK on the access points automatically:

```
Router (config-if)# mobility tcp adjust-mss
Router (config-if)#
```

Related Commands

Command	Description
ip tcp adjust-mss	Adjusts the MSS value of TCP SYN packets going through a router.
show mobility	Displays information about the Layer 3 mobility and the wireless network.

mode

To set the redundancy mode, use the **mode** command.

mode {**rpr** | **rpr-plus** | **sso**}

Syntax Description

rpr	Specifies RPR mode.
rpr-plus	Specifies RPR+ mode.
sso	Specifies SSO mode.

Command Default

The defaults are as follows:

- SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- RPR mode if different versions are installed.
- If redundancy is enabled, the default is the mode that you have configured.

Command Modes

Redundancy configuration

Command History

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

Usage Guidelines

The **rpr-plus** keywords are not supported by the Supervisor Engine 32 PISA.

NSF with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, IPX, and MPLS.

If you have configured MPLS on the Catalyst 6500 series switch with redundant supervisor engines, you must configure the Catalyst 6500 series switch in RPR mode. The switch should not be running in the default mode of SSO.

Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

The standby supervisor engine reloads on any change of mode and begins to work in the current mode.

Examples

This example shows how to set the redundancy mode to SSO:

```
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)#
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.
route-converge-interval	Configures the time interval after which the old FIB entries are purged.
show redundancy	Displays RF information.
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

mode dot1q-in-dot1q access-gateway

To enable a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation, use the **mode dot1q-in-dot1q access-gateway** command. To disable the QinQ VLAN translation on the interface, use the **no** form of this command.

mode dot1q-in-dot1q access-gateway

no mode dot1q-in-dot1q access-gateway

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is supported on the Gigabit Ethernet WAN interfaces on Catalyst 6500 series switches that are configured with an OSM-2+4GE-WAN+ OSM module only.

802.1Q provides a trunking option that tags packets with two VLAN tags to allow multiple VLANs to be trunked together across an intermediate network. This use of a double-tagged tunnel is also referred to as QinQ tunneling.

The **mode dot1q-in-dot1q access-gateway** command enhances QinQ tunneling by tagging packets with two VLAN tags to allow multiple VLANs to be trunked together across an intermediate network. A double-tagged tunnel performs the following functions:

- Switches packets that are tagged with two 802.1Q VLAN tags to a destination service that is based on a combination of VLAN tags.
- Supports traffic shaping based on the VLAN tags.
- Copies the 802.1P prioritization bits (P bits) from the inner (customer) VLAN tag to the outer (service provider) VLAN tag.

You can also combine multiple GE-WAN interfaces into a virtual port-channel interface to enable QinQ link bundling. Combining the interfaces not only simplifies the configuration but allows the GE-WAN OSM to load balance the PE VLANs among the physical interfaces that are members of the bundle. In addition, if one interface member of the link bundle goes down, its PE VLANs are automatically reallocated to the other members of the bundle.

Note You must remove all IP addresses that have been configured on the interface before using the **mode dot1q-in-dot1q access-gateway** command.

After configuring the **mode dot1q-in-dot1q access-gateway** command, use the **bridge-domain (subinterface configuration)** command to configure the VLAN mapping to be used on each subinterface.

Caution Using the **mode dot1q-in-dot1q access-gateway** command on an interface automatically deletes all the subinterfaces that might be configured on the interface. It also releases any internal VLANs that might have been previously used on the interface and its subinterfaces, allowing them to be reused for QinQ translation. Using the **no** form of the command deletes all subinterfaces and releases any VLANs that are currently being used by the interface and subinterface. We recommend that you save the interface configuration before entering the **mode dot1q-in-dot1q access-gateway** command.

Note Port-channel interface counters (as 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.

Tip The **mls qos trust** command has no effect on a GE-WAN interface or port-channel group that has been configured with the **mode dot1q-in-dot1q access-gateway** command. These interfaces and port channels always trust the VLAN CoS bits in this configuration.

Examples

This example shows a typical configuration for the **mode dot1q-in-dot1q access-gateway** command:

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

This example shows the system message that appears when you try to configure the **mode dot1q-in-dot1q access-gateway** command without first removing the IP address configuration:

```
Router# configure terminal
Router(config)# interface GE-WAN 3/0
Router(config-if)# mode dot1q-in-dot1q access-gateway

% interface GE-WAN3/0 has IP address 192.168.100.101
configured. Please remove the IP address before configuring
'mode dot1q-in-dot1q access-gateway' on this interface.

Router(config-if)# no ip address 192.168.100.101 255.255.255
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

This example shows how to disable QinQ mapping on an interface by using the **no** form of the **mode dot1q-in-dot1q access-gateway** command. In addition, this command automatically removes all subinterfaces on the interface and all of the subinterface QinQ mappings (configured with the **bridge-domain (subinterface configuration)** command) and service policies.

```
Router# configure terminal
Router(config)# interface GE-WAN 3/0
Router(config-if)# no mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

This example shows a virtual port-channel interface that was created and assigned with two GE-WAN interfaces. The **mode dot1q-in-dot1q access-gateway** command is then enabled on the port-channel interface to allow it to act as a QinQ link bundle:

```
Router(config)# interface port-channel 20
Router(config-if)# interface GE-WAN 3/0
Router(config-if)# port-channel 20 mode on
Router(config-if)# interface GE-WAN 3/1
Router(config-if)# port-channel 20 mode on
Router(config-if)# interface port-channel 20
Router(config-if)# no ip address
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

This example shows the error message that appears if you attempt to enable QinQ translation on a port-channel interface that contains one or more invalid interfaces:

```
Router# configure terminal
Router(config)# interface port-channel 30
7600-2(config-if)# mode dot1q-in-dot1q access-gateway

% 'mode dot1q-in-dot1q access-gateway' is not supported on Port-channel30
% Port-channel30 contains 2 Layer 2 Gigabit Ethernet interface(s)

Router(config-if)#
```

Related Commands

Command	Description
bridge-domain (subinterface configuration)	Binds a PVC to the specified *vlan-id*.
class-map	Accesses the QoS class map configuration mode to configure QoS class maps.
policy-map	Accesses QoS policy-map configuration mode to configure the QoS policy map.
service-policy	Attaches a policy map to an interface.
set cos cos-inner (policy-map configuration)	Sets the 802.1Q prioritization bits in the trunk VLAN tag of a QinQ-translated outgoing packet with the priority value from the inner customer-edge VLAN tag.

monitor event-trace (EXEC)

To control the event trace function for a specified Cisco IOS software subsystem component, use the **monitor event-trace** command.

monitor event-trace all-traces {{**continuous** [**cancel**]} | {**dump** [**merged**] [**pretty**]}}

monitor event-trace l3 {**clear** | {**continuous** [**cancel**]} | **disable** | {**dump** [**pretty**]} | **enable** | {**interface** *type mod/port*} | **one-shot**}

monitor event-trace spa {**clear** | {**continuous** [**cancel**]} | **disable** | {**dump** [**pretty**]} | **enable** | **one-shot**}

monitor event-trace subsys {**clear** | {**continuous** [**cancel**]} | **disable** | {**dump** [**pretty**]} | **enable** | **one-shot**}

Syntax Description

all-traces	Displays the configured merged-event traces.
continuous	Displays the latest event trace entries continuously.
cancel	(Optional) Cancels the continuous display of latest trace entries.
dump	Writes the event trace results to the file configured using the **monitor event-trace (global configuration)** command.
merged	(Optional) Dumps the entries in all event traces sorted by time.
pretty	(Optional) Saves the event trace message in an ASCII format.
l3	Displays information about the Layer 3 trace.
clear	Clears the trace.
disable	Turns off event tracing for the specified component.
enable	Turns on event tracing for the specified component.
interface *type mod/port*	Specifies the interface to be logged.
one-shot	Clears any existing trace information from the memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the **monitor event-trace (global configuration)** command.
spa	Displays information about the SPA trace.
subsys	Displays information about the initial trace of the subsystem.

Command Default

Trace information is saved in a binary format.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **monitor event-trace** (EXEC) command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace (global configuration)** command.

The trace messages are saved in a binary format.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace (global configuration)** command for each instance of a trace.

Cisco IOS software allows for the subsystem components to define whether support for event tracing is enabled or disabled at boot. You can enable or disable event tracing in two ways: using the **monitor event-trace** (EXEC) command or using the **monitor event-trace (global configuration)** command. To enable event tracing again, you would enter the **enable** form of either of these commands.

To determine whether a subsystem has enabled or disabled event tracing, use the **monitor event-trace ?** command to get a list of software components that support event tracing. To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to view trace messages.

Use the **show monitor event-trace** command to display trace messages.

Use the **monitor event-trace** *component* **dump** command to save trace message information for a single event. By default, trace information is saved in a binary format. If you want to save trace messages in an ASCII format, possibly for additional application processing, use the **monitor event-trace** *component* **dump pretty** command.

To write the trace messages for all events currently enabled on a networking device to a file, enter the **monitor event-trace dump-file (global configuration)** command.

To configure the file where you want to save trace information, use the **monitor event-trace (global configuration)** command.

Examples

This example shows how to stop event tracing, clear the current memory, and reenable the trace function for the SPA component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace spa disable
Router# monitor event-trace spa clear
Router# monitor event-trace spa enable
```

This example shows how you can use the **one-shot** keyword to accomplish the same function as the previous example except that you do not have to enter as many commands. Once the size of the trace message file has been exceeded, the trace is terminated.

```
Router# monitor event-trace spa one-shot
Router#
```

This example shows how to write the trace messages for an event in a binary format. The trace messages for the IPC component are written to a file as follows:

```
Router# monitor event-trace ipc dump
Router#
```

This example shows how to write the trace messages for an event in an ASCII format. In this example, the trace messages for the MBUS component are written to a file.

```
Router# monitor event-trace mbus dump pretty
Router#
```

Related Commands

Command	Description
monitor event-trace (global configuration)	Configures event tracing for a specified Cisco IOS software subsystem component.
show monitor event-trace	Displays event trace messages for Cisco IOS software subsystem components.

monitor event-trace (global configuration)

To configure event tracing for a specified Cisco IOS software subsystem component, use the **monitor event-trace** (global) command. To change the default setting to enable or disable event tracing, see the "Usage Guidelines" section for this command.

monitor event-trace all-traces dump-file *filename*

monitor event-trace l3 {**disable** | **dump-file** *filename* | **enable** | **size** *number* | {**stacktrace** [*depth*]}}

monitor event-trace sequence-number

monitor event-trace spa {**disable** | **dump-file** *filename* | **enable** | **size** *number* | {**stacktrace** [*depth*]}}

monitor event-trace stacktrace

monitor event-trace subsys {**disable** | **dump-file** *filename* | **enable** | **size** *number* | {**stacktrace** [*depth*]}}

monitor event-trace timestamps [{**datetime** [**localtime**] [**msec**] [**show-timezone**]} | **uptime**]

Syntax Description

dump-file *filename*	Specifies the URL to store the dump file containing the merged traces.
l3	Displays information about the Layer 3 trace.
disable	Turns off event tracing.
enable	Turns on event tracing.
size *number*	Sets the number of messages that can be written to memory for a single instance of a trace; valid values are from 1 to 65536 messages.
stacktrace	Displays the stack trace stored with event trace entries.
depth	(Optional) Trace call stack at tracepoints; valid values are from 1 to 16.
sequence-number	Displays the event trace entries with a sequence number.
spa	Displays information about the SPA trace.
subsys	Displays information about the initial trace of the subsystem.
timestamps	Displays information about the format of event trace time stamps.
datetime	(Optional) Displays information about the format of event trace time stamps.
localtime	(Optional) Displays information about the format of event trace time stamps and includes the date and time.
msec	(Optional) Includes milliseconds in the time stamp.
show-timezone	(Optional) Displays information about the format of event trace time stamps and includes time zone information.
uptime	(Optional) Displays time-stamped information about the system uptime.

Command Default Enabled or disabled depending on the software component.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Note Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a TAC representative. In Cisco IOS software images that do not provide subsystem support for the event trace function, the **monitor event-trace (global configuration)** command is not available.

Cisco IOS software allows the subsystem components to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows users to change the default two ways: using the **monitor event-trace (EXEC)** command or using the **monitor event-trace (global configuration)** command.

Additionally, default settings do not show up in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace** *component* **enable** command will not show up in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a line in the configuration file.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace (global configuration)** command for each instance of a trace.

When the number of event trace messages in memory exceeds the size, new messages will begin to overwrite the older messages in the file.

The maximum *filename* length (path and filename) is 100 characters and the path can point to flash memory on the networking device or to a TFTP or FTP server.

To determine whether a subsystem has enabled or disabled event tracing, use the **monitor event-trace ?** command to get a list of software components that support event tracing.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to view trace messages.

To specify the trace call stack at tracepoints, you must clear the trace buffer first.

Examples

This example shows how to stop event tracing, clear the current memory, and reenable the trace function for the SPA component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router(config)# monitor event-trace spa disable
Router(config)# monitor event-trace spa clear
Router(config)# monitor event-trace spa enable
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls the event trace function for a specified Cisco IOS software subsystem component.
show monitor event-trace	Displays event trace messages for Cisco IOS software subsystem components.

monitor permit-list

To configure a destination port permit list or add to an existing destination port permit list, use the **monitor permit-list** command. To delete from or clear an existing destination port permit list, use the **no** form of this command.

monitor permit-list

monitor permit-list destination {**interface** *type*} {*slot*/*port*[**-***port*] [**,** *type slot*/*port* **-** *port*]

no monitor permit-list

no monitor permit-list destination {**interface** *type*} {*slot*/*port*[**-***port*] [**,** *type slot*/*port* **-** *port*]

Syntax Description

destination	Specifies a destination port.
interface *type*	Specifies the interface type; valid values are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
slot/*port*	Slot and port number.
-*port*	(Optional) Range of ports.
,	(Optional) Additional interface type and range of ports.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

To prevent accidental configuration of ports as destinations, you can create a permit list of the ports that are valid for use as destinations. With a destination port permit list configured, you can only configure the ports in the permit list as destinations.

Examples

This example shows how to configure a destination port permit list that includes Gigabit Ethernet ports 5/1 through 5/4 and 6/1:

```
Router# configure terminal
Router(config)# monitor permit-list
Router(config)# monitor permit-list destination interface gigabitethernet 5/1-4,
gigabitethernet 6/1
```

Related Commands

Command	Description
show monitor permit-list	Displays the permit-list state and interfaces configured.

monitor session

To start a new ERSPAN, SPAN, or RSPAN session, add or delete interfaces or VLANs to or from an existing session, filter ERSPAN, SPAN, or RSPAN traffic to specific VLANs, or delete a session, use the **monitor session** command. To remove one or more source or destination interfaces from the session, remove a source VLAN from the session, or delete a session, use the **no** form of this command.

monitor session *session* **source** {{**interface** *type*} | {{**vlan** *vlan-id*} [**rx** | **tx** | **both**]} | {**remote vlan** *rspan-vlan-id*}}

monitor session *session* **destination** {{**interface** *type*} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*} | {**analysis-module** *slot-number*} | {**data-port** *port-number*}}

monitor session *session-number* **filter vlan** *vlan-range*

monitor session servicemodule *mod-list*

monitor session *session-number* **type** {**erspan-source | erspan-destination**}

no monitor session {{**range** *session-range*} | **local** | **remote** | **all** | *session*}

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

no monitor session *session* **destination** {{**interface** *type*} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*} | {**analysis-module** *slot-number*} | {**data-port** *port-number*}}

Syntax Description

session	Number of the SPAN session; valid values are from 1 to 66.
source	Specifies the SPAN source.
interface *type*	Specifies the interface type; see the “Usage Guidelines” section for formatting information.
vlan *vlan-id*	Specifies the VLAN ID; valid values are from 1 to 4094.
rx	(Optional) Specifies the monitor-received traffic only.
tx	(Optional) Specifies the monitor-transmitted traffic only.
both	(Optional) Specifies the monitor-received and monitor-transmitted traffic.
remote vlan *rspan-vlan-id*	Specifies the RSPAN VLAN as a destination VLAN.
destination	Specifies the SPAN-destination interface.
analysis-module *slot-number*	Specifies the network analysis module number; see the “Usage Guidelines” section for additional information.
data-port *port-number*	Specifies the data-port number; see the “Usage Guidelines” section for additional information.
filter vlan *vlan-range*	Limits SPAN-source traffic to specific VLANs.
servicemodule	Specifies service modules.
mod-list	(Optional) List of service module numbers.
type erspan-source	Enters the ERSPAN source-session configuration mode; see the **monitor session type** command for additional information.

type erspan-destination	Enters the ERSPAN destination-session configuration mode; see the **monitor session type** command for additional information.
range *session-range*	Specifies the range of sessions.
local	Specifies the local session.
remote	Specifies the remote session.
all	Specifies all sessions.

Command Default

The defaults are as follows:

- **both**.
- **servicemodule**—All service modules are allowed to use the SPAN servicemodule session.

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

Note Be careful when configuring SPAN-type source ports that are associated to SPAN-type destination ports because you do not configure SPAN on high-traffic interfaces. If you configure SPAN on high-traffic interfaces, you may saturate replication engines and interfaces. To configure SPAN-type source ports that are associated to SPAN-type destination ports, enter the **monitor session** *session* **source** {{**interface** *type*} | {{**vlan** *vlan-id*} [**rx** | **tx** | **both**]} | {**remote vlan** r*span-vlan-id*}} command.

Use these formatting guidelines when configuring monitor sessions:

- *interface* and *single-interface* formats are *type slot*/*port*; valid values for *type* are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- An *interface-list* is a list of interfaces that are separated by commas. Insert a space before and after each comma as shown in this example:

  single-interface , *single-interface* , *single-interface* ...
- An *interface-range* is a range of interfaces that are separated by dashes. Insert a space before and after each dash. To enter multiple ranges, separate each range with a comma as shown in this example:

  type slot/*first-port* - *last-port*
- A *mixed-interface-list* is a mixed list of interfaces. Insert a space before and after each dash and comma as shown in this example:

  single-interface, *interface-range* , ... in any order.
- A *single-vlan* is an ID number of a single VLAN; valid values are from 1 to 4094.
- A *vlan-list* is a list of VLAN IDs that are separated by commas. An example is shown as follows:

  single-vlan , *single-vlan* , *single-vlan* ...
- A *vlan-range* is a range of VLAN IDs that are separated by dashes. An example is shown as follows:

  first-vlan-ID - *last-vlan-ID*
- A *mixed-vlan-list* is a mixed list of VLAN IDs. Insert a space before and after each dash. To enter multiple ranges, separate each VLAN ID with a comma as shown in this example:

  single-vlan , *vlan-range* , ... in any order

The **analysis-module** *slot-number* and the **data-port** *port-number* keywords and arguments are supported on Network Analysis Modules only.

The number of valid values for **port-channel** *number* are a maximum of 64 values ranging from 1 to 256.

You cannot share the destination interfaces among SPAN sessions. For example, a single destination interface can belong to one SPAN session only and cannot be configured as a destination interface in another SPAN session.

The local SPAN, RSPAN, and ERSPAN session limits are as follows:

Total Sessions	Local SPAN, RSPAN Source, or ERSPAN Source Sessions	RSPAN Destination Sessions	ERSPAN Destination Sessions
66	2 (ingress or egress or both)	64	23

The local SPAN, RSPAN, and ERSPAN source and destination limits are as follows:

	In Each Local SPAN Session	In Each RSPAN Source Session	In Each ERSPAN Source Session	In Each RSPAN Destination Session	In Each ERSPAN Destination Session
Egress or ingress and egress sources				—	—
	128	128	128		
Ingress sources				—	—
	128	128	128		
RSPAN and ERSPAN destination session sources	—	—	—	1 RSPAN VLAN	1 IP address
Destinations per session	64	1 RSPAN VLAN	1 IP address	64	64

A particular SPAN session can either monitor the VLANs or monitor individual interfaces—you cannot have a SPAN session that monitors both specific interfaces and specific VLANs. If you first configure a SPAN session with a source interface, and then try to add a source VLAN to the same SPAN session, you get an error. You also get an error if you configure a SPAN session with a source VLAN and then try to add a source interface to that session. You must first clear any sources for a SPAN session before switching to another type of source.

If you enter the **filter** keyword on a monitored trunk interface, only traffic on the set of specified VLANs is monitored.

The port-channel interfaces display in the list of **interface** options if you have them configured. The VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session** *session* **source vlan** *vlan-id* command.

The **show monitor** command displays the SPAN servicemodule session only if it is allocated in the system. It also displays a list of allowed modules and a list of active modules that can use the servicemodule session.

Only the **no** form of the **monitor session servicemodule** command is displayed when you enter the **show running-config** command.

If no module is allowed to use the servicemodule session, the servicemodule session is automatically deallocated. If at least one module is allowed to use the servicemodule session and at least one module is online, the servicemodule session is automatically allocated.

If you allow or disallow a list of modules that are not service modules from using the servicemodule session, there will be no effect on the allocation or deallocation of the servicemodule session. Only the list of modules is saved in the configuration.

If you disable the SPAN servicemodule session with the **no monitor session servicemodule** command, allowing or disallowing a list of modules from using the servicemodule session has no effect on the allocation or deallocation of the servicemodule session. Only the list of modules is saved in the configuration.

The **monitor session servicemodule** command is accepted even if there are no modules physically inserted in any slot.

Examples

This example shows how to configure multiple sources for a session:

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to configure an RSPAN destination in the final switch (RSPAN destination session):

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```

This example shows how to clear the configuration for sessions 1 and 2:

```
Router(config)# no monitor session 1 - 2
Router(config)#
```

This example shows how to clear the configuration for all sessions:

```
Router(config)# no monitor session all
Router(config)#
```

This example shows how to clear the configuration for all remote sessions:

```
Router(config)# no monitor session remote
Router(config)#
```

This example shows how to allow a list of modules to use the SPAN servicemodule session:

```
Router(config)# monitor session servicemodule module 1-2
Router(config)#
```

This example shows how to disallow a list of modules from using the SPAN servicemodule session:

```
Router(config)# no monitor session servicemodule module 1-2
Router(config)#
```

Related Commands

Command	Description
remote-span	Configures a VLAN as an RSPAN VLAN.
show monitor session	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

monitor session type

To create an ERSPAN source session number or enter the ERSPAN session configuration mode for the session, use the **monitor session type** command. To remove one or more source or destination interfaces from the ERSPAN session, use the **no** form of this command.

monitor session *erspan-session-number* **type** {**erspan-destination** | **erspan-source**}

no monitor session *erspan-session-number* **type** {**erspan-destination** | **erspan-source**}

Syntax Description

erspan-session-number	Number of the SPAN session; valid values are from 1 to 66.
type erspan-destination	Specifies the ERSPAN destination-session configuration mode.
type erspan-source	Specifies the ERSPAN source-session configuration mode.

Command Modes

This command has no default settings.

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

ERSPAN is supported on hardware revision 3.2 or higher. Enter the **show module version | include WS-SUP720-BASE** command to display the hardware revision.

ERSPAN traffic is GRE-encapsulated SPAN traffic that can only be processed by an ERSPAN destination session.

All ERSPAN source sessions on a switch must use the same source IP address. You enter the **origin ip address** command to configure the IP address for the ERSPAN source sessions.

All ERSPAN destination sessions on a switch must use the same IP address. You enter the **ip address** command to configure the IP address for the ERSPAN destination sessions. If the ERSPAN destination IP address is not a Supervisor Engine 32 PISA (for example, it is a network sniffer), the traffic arrives with the GRE and RSPAN headers/encapsulation intact.

The ERSPAN source session destination IP address, which must be configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to the destination ports. You configure the same address in both the source and destination sessions with the **ip address** command.

The ERSPAN ID differentiates the ERSPAN traffic arriving at the same destination IP address from different ERSPAN source sessions.

The local ERSPAN session limits are as follows:

- Total sessions—66
- Source sessions—2 (ingress or egress or both)
- Destination sessions—23

The **monitor session type** command creates a new ERSPAN session or allows you to enter the ERSPAN session configuration mode. ERSPAN uses separate source and destination sessions. You configure the source and destination sessions on different switches. The ERSPAN session configuration mode prompts are as follows:

- Router(config-mon-erspan-src)—Indicates the ERSPAN source session configuration mode.
- Router(config-mon-erspan-src-dst)—Indicates the ERSPAN source session destination configuration mode.
- Router(config-mon-erspan-dst)—Indicates the ERSPAN destination session configuration mode.
- Router(config-mon-erspan-dst-src)—Indicates the ERSPAN destination session source configuration mode

Table 2-25 lists the ERSPAN destination session configuration mode syntaxes.

Table 2-25 ERSPAN Destination Session Configuration Mode Syntaxes

Syntax	Description
Global Configuration Mode	
monitor session *erspan-destination-session-number* **type erspan-destination**	Enters ERSPAN destination session configuration mode and changes the prompt to the following: `Router(config-mon-erspan-dst)#`
Destination Session Configuration Mode	
description *session-description*	(Optional) Describes the ERSPAN destination session.
shutdown	(Optional) (Default) Inactivates the ERSPAN destination session.
no shutdown	Activates the ERSPAN destination session.
destination {*single-interface* | *interface-list* | *interface-range* | *mixed-interface-list*}	Associates the ERSPAN destination session number with the destination ports.
source	Enters ERSPAN destination session source configuration mode and changes the prompt to the following: `Router(config-mon-erspan-dst-src)#`
Destination Session Source Configuration Mode	
ip address *ip-address* [**force**]	Configures the ERSPAN flow destination IP address, which must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.
erspan-id *erspan-flow-id*	Configures the ID number used by the destination and destination sessions to identify the ERSPAN traffic.
vrf *vrf-name*	(Optional) Configures the VRF name of the packets in the ERSPAN traffic.

Table 2-26 lists the ERSPAN source session configuration mode syntaxes.

Table 2-26 ERSPAN Source Session Configuration Mode Syntaxes

Syntax	Description
Global Configuration Mode	
monitor session *erspan-source-session-number* **type erspan-source**	Enters ERSPAN source session configuration mode and changes the prompt to the following: `Router(config-mon-erspan-src)#`
Source Session Configuration Mode	
description *session-description*	(Optional) Describes the ERSPAN source session.
shutdown	(Optional) (Default) Inactivates the ERSPAN source session.
no shutdown	Activates the ERSPAN source session.
source {{*single-interface* | *interface-list* | *interface-range* | *mixed-interface-list* | *single-vlan* | *vlan-list* | *vlan-range* | *mixed-vlan-list*} [**rx** | **tx** | **both**]}	Associates the ERSPAN source session number with the source ports or VLANs, and selects the traffic direction to be monitored.
filter {*single-vlan* | *vlan-list* | *vlan-range* | *mixed-vlan-list*}	(Optional) Configures source VLAN filtering when the ERSPAN source is a trunk port.
destination	Enters ERSPAN source session destination configuration mode and changes the prompt to the following: `Router(config-mon-erspan-src-dst)#`
Source Session Destination Configuration Mode	
ip address *ip-address*	Configures the ERSPAN flow destination IP address, which must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.
erspan-id *erspan-flow-id*	Configures the ID number used by the source and destination sessions to identify the ERSPAN traffic.
origin ip address *ip-address*	Configures the IP address used as the source of the ERSPAN traffic.
ip {{**ttl** *ttl-value*} | {**prec** *ipp-value*} | {**dscp** *dscp-value*}}	(Optional) Configures the following packet values in the ERSPAN traffic: • **ttl** *ttl-value*—IP time-to-live (TTL) value • **prec** *ipp-value*—IP-precedence value • **dscp** *dscp-value*—IP-precedence value
vrf *vrf-name*	(Optional) Configures the VRF name of the packets in the ERSPAN traffic.

When you configure the monitor sessions, follow these syntax guidelines:

- *erspan-destination-span-session-number* can range from 1 to 66.
- *single-interface* is **interface** *type slot*/*port*; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.

- *interface-list* is *single-interface* , *single-interface* , *single-interface* ...

Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface-range* is **interface** *type slot/first-port - last-port* .
- *mixed-interface-list* is, in any order, *single-interface* , *interface-range* , ...
- *erspan-flow-id* can range from 1 to 1023.

When you clear the monitor sessions, follow these syntax guidelines:

- The **no monitor session** *session-number* command entered with no other parameters clears the session *session-number.*
- *session-range* is *first-session-number-last-session-number.*

Note When you enter the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

Examples

This example shows how to configure an ERSPAN source session number and enter the ERSPAN source session configuration mode for the session:

```
Router(config)# monitor session 55 type erspan-source
Router(config-mon-erspan-src)#
```

This example shows how to configure an ERSPAN destination session number and enter the ERSPAN destination session configuration mode for the session:

```
Router(config)# monitor session 55 type erspan-destination
Router(config-mon-erspan-dst)#
```

This example shows how to associate the ERSPAN destination session number with the destination ports:

```
Router(config-mon-erspan-dst) destination interface fastethernet 1/2 , 2/3
```

This example shows how to enter the ERSPAN destination session source configuration:

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

This example shows how to enter the ERSPAN destination session source configuration mode:

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

This example shows how to configure multiple sources for a session:

```
Router(config-mon-erspan-src)# source interface fastethernet 5/15 , 7/3 rx
Router(config-mon-erspan-src)# source interface gigabitethernet 1/2 tx
Router(config-mon-erspan-src)# source interface port-channel 102
Router(config-mon-erspan-src)# source filter vlan 2 - 3
Router(config-mon-erspan-src)#
```

This example shows how to enter the ERSPAN source session destination configuration mode:

```
Router(config-mon-erspan-src)# destination
Router(config-mon-erspan-src-dst)#
```

This example shows how to configure the ID number that is used by the source and destination sessions to identify the ERSPAN traffic:

```
Router(config-mon-erspan-src-dst)# erspan-id 1005
Router(config-mon-erspan-src-dst)#
```

Related Commands

Command	Description
show monitor session	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

mpls l2transport route

To enable routing of Layer 2 packets over MPLS, use the **mpls l2transport route** command. To disable routing over MPLS, use the **no** form of this command.

mpls l2transport route *destination vc-id*

no mpls l2transport route *destination vc-id*

Syntax Description

destination	IP address of the router to which the virtual circuit is destined.
vc-id	Virtual-circuit identification to a router.

Command Modes

This command has no default settings.

Command Default

Interface configuration

Command History

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

Usage Guidelines

The **mpls l2transport route** command enables the virtual connection used to route the VLAN packets. The types of virtual connections used are as follows:

- VC Type 4—Allows all the traffic in a VLAN to use a single VC across the MPLS network.
- VC Type 5—Allows all traffic on a port to share a single VC across the MPLS network.

During the VC setup, VC type 5 is advertised. If the peer advertises VC type 4, the VC type is changed to type 4 and the VC is restarted. Note that the change only happens from type 5 to type 4 and never from type 4 to type 5.

An MPLS VLAN virtual circuit in Layer 2 runs across an MPLS cloud to connect the VLAN interfaces on two PE routers.

Use the **mpls l2transport route** command on the VLAN interface of each PE router to route the VLAN packets in Layer 2 across the MPLS cloud to the VLAN interface of the other PE router. Specify the IP address of the other PE router for the destination parameter. Do not specify the IP address of the router from which you are issuing the command.

You can choose any value for the virtual-connection ID. However, the virtual-circuit ID must be unique to the virtual connection. In large networks, you may need to track the virtual-connection ID assignments to ensure that a virtual-connection ID does not get assigned twice.

The routed virtual connections are supported on the main interfaces, not subinterfaces.

The virtual-circuit ID must be unique to each virtual connection.

Examples

This example shows how to enable routing of Layer 2 packets over MPLS:

```
Router(config-if)# mpls l2transport route 192.16.0.1
Router(config-if)#
```

Related Commands

Command	Description
show mpls l2transport vc	Displays the state of virtual circuits on a router.

mpls load-balance per-label

To enable the load balancing for the tag-to-tag traffic, use the **mpls load-balance per-label** command. To return to the default settings, use the **no** form of this command.

mpls load-balance per-label

no mpls load-balance per-label

Syntax Description

This command has no arguments or keywords.

Command Modes

Disabled

Command Default

Global configuration (config)

Command History

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

Usage Guidelines

When you enable load balancing for the tag-to-tag traffic, the traffic is balanced based on the incoming label (per prefix) among MPLS interfaces. Each MPLS interface supports an equal number of incoming labels.

You can use the **show mpls ttfib** command to display the incoming label (indicated by an asterisk) that is included in the load balancer.

Examples

This example shows how to enable the load balancing for the tag-to-tag traffic:

```
Router(config)# mpls load-balance per-label
Router(config)#
```

This example shows how to disable the load balancing for the tag-to-tag traffic:

```
Router(config)# no mpls load-balance per-label
Router(config)#
```

Related Commands

Command	Description
show mpls ttfib	Displays information about the MPLS TTFIB table.

mpls ttl-dec

To specify standard MPLS tagging, use the **mpls ttl-dec** command. To return to the default settings, use the **no** form of this command.

mpls ttl-dec

no mpls ttl-dec

Syntax Description

This command has no arguments or keywords.

Command Modes

Optimized MPLS tagging (**no mpls ttl-dec**).

Command Default

Interface configuration

Command History

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

Usage Guidelines

MPLS tagging has been optimized to allow the rewriting of the original packet's IP ToS and TTL values before the MPLS label is pushed onto the packet header. This change can result in a slightly lower performance for certain types of traffic. If the packet's original ToS/TTL values are not significant, you enter the **mpls ttl-dec** command for standard MPLS tagging.

Examples

This example shows how to configure the Catalyst 6500 series switch to use standard MPLS tagging behavior:

```
Router(config)# mpls ttl-dec
Router(config)#
```

This example shows how to configure the Catalyst 6500 series switch to use optimized MPLS tagging behavior:

```
Router(config)# no mpls ttl-dec
Router(config)#
```

Related Commands

Command	Description
mpls l2transport route	Enables routing of Layer 2 packets over MPLS.

mtu

To adjust the maximum packet size or MTU size, use the **mtu** command. To return to the default settings, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	Byte size; valid values are from 64 to 9216 for SVI ports, from 1500 to 9170 for the GE-WAN+ ports, and from 1500 to 9216 for all other ports.

Command Modes

Table 2-27 lists the default MTU values if you disable the jumbo frames.

Table 2-27 Default MTU Values

Media Type	Default MTU (bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

If you enable the jumbo frames, the default is 64 for the SVI ports and 9216 for all the other ports. The jumbo frames are disabled by default.

Command Default

Interface configuration

Command History

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

Usage Guidelines

For switch ports, only one larger-than-default MTU value is allowed globally. For Layer 3 ports, including router ports and VLANs, you can configure nondefault MTU values on a per-interface basis.

For a complete list of modules that do not support jumbo frames, refer to the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY*.

Changing the MTU value with the **mtu** command can affect values for the protocol-specific versions of the command (for example, the **ip mtu** command). If the values that are specified with the **ip mtu** command are the same as the value that is specified with the **mtu** command, and you change the value for the **mtu** command, the **ip mtu** value automatically matches the new **mtu** command value. However, changing the values for the **ip mtu** command has no effect on the value for the **mtu** command.

Examples

This example shows how to specify an MTU of 1800 bytes:

```
Router(config)# interface fastethernet 5/1
Router(config-if)#  mtu 1800
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.

name (MST configuration submode)

To set the name of an MST region, use the **name** command. To return to the default name, use the **no** form of this command.

name *name*

no name *name*

Syntax Description

name	Name to give the MST region. It can be any string with a maximum length of 32 characters.

Command Modes

Empty string

Command Default

MST configuration submode

Command History

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

Usage Guidelines

Two or more Catalyst 6500 series switches with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

Caution Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the Catalyst 6500 series switch in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
Router(config-mst)# name Cisco
Router(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
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.

neighbor

To specify the type of tunnel signaling and encapsulation mechanism for each peer, use the **neighbor** command. To disable a split horizon, use the **no** form of this command.

neighbor *remote-router-id* {**encapsulation** *encapsulation-type*} | {**pw-class** *pw-name*} [**no-split-horizon**]

no neighbor *remote-router-id*

Syntax Description

remote-router-id	Remote peering router identification.
encapsulation *encapsulation*	Specifies the tunnel encapsulation type; valid values are **l2tpv3** and **mpls**.
pw-class *pw-name*	Specifies the pseudo-wire property to be used to set up the emulated VC.
no-split-horizon	(Optional) Disables the Layer 2 split horizon in the data path.

Command Modes

Split horizon is enabled.

Command Default

Layer 2 VFI manual configuration submode

Command History

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

To avoid looping, you should not disable a split horizon in a fully meshed Virtual PVLAN service (VPLS) network.

Examples

This example shows how to specify the tunnel encapsulation type:

```
Router(config-vfi)# neighbor 333 encapsulation mpls
Router(config-vfi)#
```

This example shows how to disable the Layer 2 split horizon in the data path:

```
Router(config-vfi)# neighbor 333 no-split-horizon
Router(config-vfi)#
```

net

To configure an IS-IS NET for the routing process, use the **net** command. To remove a NET, use the **no** form of this command.

net *net1* {**alt** *net2*}

no net *net*

Syntax Description

net1	NET NSAP name or address for the IS-IS routing process on the PISA in the primary slot; see the "Usage Guidelines" section for additional information.
alt *net2*	Specifies the NET name or address for the IS-IS routing process on the PISA in the alternate slot; see the "Usage Guidelines" section for additional information.
net	NET NSAP name or address to be removed.

Command Default

The defaults are as follows:

- No NET is configured.
- IS-IS process is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

A NET is an NSAP where the last byte is always the n-selector and is always zero. A NET can be from 8 to 20 bytes.

Under most circumstances, you should configure one NET only.

When entering the *net*, use these guidelines:

- In a 3-slot chassis, slot 1 is the primary slot and slot 2 is the alternate slot.
- In a 6-slot chassis, slot 5 is the primary slot and slot 6 is the alternate slot.
- In a 9-slot chassis, slot 5 is the primary slot and slot 6 is the alternate slot.
- In a 13-slot chassis, slot 7 is the primary slot and slot 8 is the alternate slot.

If you are using IS-IS to perform IP routing only (no connectionless network service routing is enabled), you must configure a NET to define the router ID and area ID.

Multiple NETs per router are allowed with a maximum of three NETs. In rare circumstances, you can configure two or three NETs. In such a case, the area this router is in will have three area addresses and only one area.

Multiple NETs can be temporarily useful for network reconfiguration where multiple areas are merged, or where one area is split into more areas. Multiple area addresses enable you to renumber an area individually as needed.

Examples

This example shows how to configure a router with system ID 0000.0c11.1110 and area ID 47.0004.004d.0001:

```
router isis Pieinthesky
 net 47.0004.004d.0001.0001.0c11.1111.00
```

This example shows three IS-IS routing processes with three areas that are configured. Each area has a unique identifier, but the system ID is the same for all areas.

```
clns routing

...

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB
 clns router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
 clns router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02
 clns router isis A3253-02

...

router isis BB                          ! Defaults to "is-type level-1-2"
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

Related Commands

Command	Description
is-type	Configures the routing level for an instance of the IS-IS routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

nsf

To enable and configure Cisco NSF, use the **nsf** command. To disable NSF, use the **no** form of this command.

nsf [**enforce global**]

nsf [{**cisco** | **ietf**} | {**interface** {**wait** *seconds*}} | {**interval** *minutes*} | {**t3** [**adjacency** | {**manual** *seconds*}}]

no nsf

Syntax Description

enforce global	(Optional) Cancels OSPF NSF restart when non-NSF-aware neighbors are detected.
cisco	(Optional) Specifies the Cisco proprietary IS-IS NSF method of checkpointing if the active RP fails over.
ietf	(Optional) Specifies the IETF IS-IS NSF method of protocol modification if the active RP fails over.
interface wait *seconds*	(Optional) Specifies how long to wait for an interface to come up after failover before it proceeds with the Cisco NSF process; valid values are from 1 to 60 seconds.
interval *minutes*	(Optional) Specifies how long to wait after a route processor stabilizes before restarting; valid values are from 0 to 1440 minutes.
t3 adjacency	(Optional) Specifies that the time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover.
t3 manual *seconds*	(Optional) Specifies the time to wait after the NSF database synchronizes before informing other nodes to remove the restarting node from consideration as a transit; valid values are from 5 to 3600 seconds.

Command Default

The default settings are as follows:

- NSF is disabled.
- **enforce global**—Enabled.
- **interval** *minutes*—5 minutes.
- **interface wait** *seconds*—10 seconds.
- **t3 manual** *seconds*—30 seconds.

Command Modes

Router configuration IS-IS

Command History

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

Usage Guidelines

The **nsf interface wait** command can be used if Cisco proprietary IS-IS NSF is configured or if the Internet Engineering Task Force (IETF) IS-IS NSF is enabled using the **nsf t3** manual command. You can use this command if an interface is slow to come up.

Note Cisco NSF is required only if the Catalyst 6500 series switch is expected to perform Cisco NSF during a restart. If the Catalyst 6500 series switch is expected to cooperate with a neighbor that is doing a Cisco NSF restart only, the switch must be NSF capable by default (running a version of code that supports Cisco NSF), but Cisco NSF does not have to be configured on the switch.

The **nsf** commands are a subset of the **router** command and affects all the interfaces that are covered by the designated process. Cisco NSF supports the BGP, OSPF, IS-IS, and EIGRP protocols. The configuration commands that enable NSF processing are as follows:

- **nsf** under the **router ospf** command
- **nsf ietf** under the **router isis** command
- **bgp graceful-restart** under the **router bgp** command

These commands must be issued as part of the router's running configuration. During the restart, these commands are restored to activate the NSF processing.

The [{**cisco** | **ietf**} | {**interface** {**wait** *seconds*}} | {**interval** *minutes*} | {**t3** [**adjacency** | {**manual** *seconds*}}] keywords and arguments apply to IS-IS only.

The {**enforce global**} keywords apply to OSPF only.

BGP NSF Guidelines

BGP support in NSF requires that neighbor networking devices be NSF-aware devices; that is, they must have the graceful restart capability and advertise that capability in the OPEN message during session establishment. If an NSF-capable router discovers that a particular BGP neighbor does not have the graceful restart capability enabled, it will not establish an NSF-capable session with that neighbor. All other neighbors that have a graceful restart capability will continue to have NSF-capable sessions with this NSF-capable networking device. Enter the **bgp graceful-restart** router configuration command to enable the graceful restart capability. Refer to the *Cisco IOS Release 12.2 Command Reference* for more information.

EIRGP NSF Guidelines

A router may be an NSF-aware router but may not be participating in helping out the NSF restarting neighbor because it is coming up from a cold start.

IS-IS NSF Guidelines

If you configure IETF on the networking device, but neighbor routers are not IETF-compatible, NSF will abort after the switchover.

Use these two keywords when configuring IS-IS NSF:

- **ietf**—Internet Engineering Task Force IS-IS—After a supervisor engine switchover, the NSF-capable router sends the IS-IS NSF restart requests to the neighboring NSF-aware devices.
- **cisco**—Cisco IS-IS. Full adjacency and LSP information is saved (checkpointed) to the standby supervisor engine. After a switchover, the newly active supervisor engine maintains its adjacencies using the checkpointed data to quickly rebuild its routing tables.

OSPF NSF Guidelines

OSPF NSF requires that all neighbor networking devices be NSF-aware devices. If an NSF-capable router discovers that it has non-NSF aware neighbors on a particular network segment, it will disable the NSF capabilities for that segment. The other network segments that are composed entirely of NSF-capable or NSF-aware routers will continue to provide NSF capabilities.

OSPF NSF supports NSF/SSO for IPv4 traffic only. OSPFv3 is not supported with NSF/SSO. Only OSPFv2 is supported with NSF/SSO.

Examples

This example shows how to enable NSF for all OSPF-process interfaces:

```
Router(config)# router ospf 109
Router(config-router)# nsf
Router(config-router)#
```

This example shows how to disable NSF for all OSPF-process interfaces:

```
Router(config)# router ospf 109
Router(config-router)# no nsf
Router(config-router)#
```

Related Commands

Command	Description
router	Enables a routing process.

pagp learn-method

To learn the input interface of the incoming packets, use the **pagp learn-method** command. To return to the default settings, use the **no** form of this command.

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

no pagp learn-method

Syntax Description

aggregation-port	Specifies how to learn the address on the port channel.
physical-port	Specifies how to learn the address on the physical port within the bundle.

Command Default

aggregation-port method

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to set the learning method to learn the address on the physical port within the bundle:

```
Router(config-if)# pagp learn-method physical-port
Router(config-if)#
```

This example shows how to set the learning method to learn the address on the port channel within the bundle:

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

Related Commands

Command	Description
show pagp	Displays port-channel information.

pagp port-priority

To select a port in hot standby mode, use the **pagp port-priority** command. To return to the default settings, use the **no** form of this command.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

priority	Priority number; valid values are from 1 to 255.

Command Default

priority is **128**.

Command Default

Interface configuration

Command History

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

Usage Guidelines

The higher the priority means the better the chances are that the port will be selected in the hot standby mode.

Examples

This example shows how to set the port priority:

```
Router(config-if)# pagp port-priority 45
Router(config-if)#
```

Related Commands

Command	Description
pagp learn-method	Learns the input interface of the incoming packets.
show pagp	Displays port-channel information.