mls exclude protocol

To specify the interface protocol to exclude from shortcutting, use the **mls exclude protocol** command. Use the **no** form of this command to remove a prior entry.

mls exclude protocol {{**both** | **tcp** | **udp**}{**port** *port-number*}}

no mls exclude

Syntax Description

both	Specifies both UDP and TCP.
tcp	Excludes TCP interfaces from shortcutting.
udp	Specifies UDP interfaces from shortcutting.
port *port-number*	Specifies the port number; valid values are from 1 to 65535.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure MLS to exclude UDP on port 69:

```
Router(config)# mls exclude protocol udp port 69
Router(config)#
```

Related Commands

show mls ip multicast
show mls ipx

mls flow

To configure the NDE flow mask, use the **mls flow** command. This command collects statistics for the supervisor engine. Use the **no** form of this command to restore the flow mask to the default settings.

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

mls flow {**ipx** {**destination** | **destination-source**}}

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

Syntax Description

ip	Enables the flow mask for MLS IP 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.
source-only	Uses all the information in the source flow mask only.
interface-full	Uses all the information in the full flow mask and the source VLAN number as the keys to the Layer 3 table.
ipx	Enables the flow mask for MLS IPX packets.

Defaults

The minimum (least specific) flow mask is the default. In systems configured with a Supervisor Engine 2, the minimum flow mask is **destination**.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(13)E	This command was changed to add the **interface-destination-source** and **interface-full** options.

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

show mls netflow

mls ip

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

mls ip

no mls ip

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(12c)E	Support for this command was introduced on the Cisco 7600 series router Supervisor Engine 2.

Examples

This example shows how to enable MLS IP shortcuts:

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

Related Commands

mls rp ip (interface configuration mode)
show mls ip multicast

mls ip cef arp-throttling

To enable per-destination based rate limiting of packets requiring ARP resolution, use the **mls ip cef arp-throttling** command. Use the **no** form of this command to disable ARP throttling.

mls ip cef arp-throttling

no mls ip cef arp-throttling

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)E1	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

ARP throttling limits the rate at which packets destined to a connected network are forwarded to the route processor. Most of these packets are dropped, but a small number are sent to the router (rate limited).

Examples

This example shows how to enable per-destination based rate limiting of packets requiring ARP resolution:

```
Router(config)# mls ip cef arp-throttling
Router(config)#
```

This example shows how to disable per-destination based rate limiting of packets requiring ARP resolution:

```
Router(config)# no mls ip cef arp-throttling
Router(config)#
```

mls ip cef load-sharing full

To set CEF load balancing to include Layer 4 ports and source IP/destination IP addresses (Layer 3), use the **mls ip cef load-sharing full** command. Use the **no** form of this command to return to the default settings.

mls ip cef load-sharing full

no mls ip cef load-sharing full

Syntax Description

This command has no arguments or keywords.

Defaults

Load balancing is based on the source IP/destination IP addresses only.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11b)E	Support for this command was introduced on the Supervisor Engine 2.

Usage Guidelines

The **mls ip cef load-sharing full** command is supported on systems configured with the Supervisor Engine 2 only.

For additional guidelines, refer to the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

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

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

This example shows how to return to the default settings:

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

Related Commands

show running-config

mls ip cef rate-limit

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

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.

Defaults

No rate limit is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

The **mls ip cef rate-limit** command is supported on systems configured with the Supervisor Engine 2 only.

Certain denial-of-service attacks target the route processing engines of routers. Certain packets that cannot be forwarded by the PFC2 are directed to the MSFC2 for processing. Denial-of-service attacks can overload the route processing engine and cause routing instability when running dynamic routing protocols. The **mls ip cef rate-limit** command can be used to limit the amount of traffic sent to the MSFC2 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 handling of packets destined to the IP addresses of the local interfaces and packets requiring 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 *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to enable and set the rate-limiting feature:

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

mls ip directed-broadcast

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

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

no mls ip directed-broadcast

Syntax Description

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

Defaults

Hardware switching of IP-directed broadcasts is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11b)E	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

This command is supported in Cisco 7600 series routers configured with a Supervisor Engine 2 with a Layer 3 Switching Engine II (PFC2) only.

You must configure jumbo-frame support to support fragmented traffic with directed broadcasts by performing one of the following:

- Enter the **mtu** command on the IP-directed broadcast interface if jumbo frames are required.
- Enter the **mls ip directed-broadcast include-router** command to forward the IP-directed broadcast packet in hardware to all hosts in the VLAN including the router.

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 hardware forwarded; they are handled at the process level by the MSFC2. The MSFC2 decision to forward or not forward the packet is then 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 secondary IP addresses of interfaces.

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

You can configure 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 you can 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 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 hardware to all hosts in the VLAN:

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

Related Commands

mls ip directed-broadcast (refer to the *Cisco IOS Release 12.1 Command Reference*)
mtu
show mls cef adjacency

mls ip inspect

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

mls ip inspect *acl-name*

no mls ip inspect *acl-name*

Syntax Description

acl-name	ACL name.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

On a Cisco 7600 series router, 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)#
```

Usage Guidelines

ip inspect (refer to the *Cisco IOS Release 12.1 Command Reference*)

mls ip multicast (global configuration mode)

To globally enable MLS IP on the Cisco 7600 series router, use the **mls ip multicast** command. Use the **no** form of this command to disable MLS IP on the Cisco 7600 series router.

mls ip multicast

no mls ip multicast

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to enable MLS IP shortcuts:

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

Related Commands

mls rp ip (global configuration mode)
show mls ip multicast

mls ip multicast (interface configuration mode)

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

mls ip multicast

no mls ip multicast

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(19)E1	Support for this command was extended to the FlexWAN module ATM subinterfaces

Examples

This example shows how to enable MLS IP shortcuts:

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

Related Commands

show mls ip multicast

mls ip multicast connected

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

mls ip multicast connected

no mls ip multicast connected

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

The **mls ip multicast connected** command is supported on systems configured with the Supervisor Engine 2 only.

Examples

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

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

Related Commands

mls ip multicast (global configuration mode)
show mls ip multicast

mls ip multicast consistency-check

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

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*	Specifies the period between scans; valid values are from 2 to 3600 seconds.

Defaults

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

Command History

Release	Modification
12.1(12c)E4	Support for this command was introduced on the Supervisor Engine 2.

Usage Guidelines

oif 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

show mls ip multicast consistency-check

mls ip multicast non-rpf-netflow (global configuration mode)

To enable the NetFlow-based non-RPF feature, use the **mls ip multicast non-rpf-netflow** command. Use the **no** form of this command to disable the feature.

mls ip multicast non-rpf-netflow

no mls ip multicast non-rpf-netflow

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

An RPF interface is used if a unicast packet is sent back to the source.

If a multicast packet encounters an RPF MFD shortcut, it is not sent to the route processor on the MSFC. The router processor never sees a copy of the packet forwarded by the hardware. The RPF MFDs are installed to switch packets arriving on the RPF interface.

A non-RPF MFD is an MFD that is installed to switch packets on the non-RPF VLAN. With RPF MFDs, the packets arriving on the RPF VLAN are forwarded to the outgoing VLANs. With non-RPF MFDs, the packets are bridged only on the VLAN on which it was received. The packet is not sent to the MSFC.

Examples

This example shows how to enable the NetFlow-based non-RPF feature:

```
Router(config)# mls ip multicast non-rpf-netflow
Router(config)#
```

Related Commands

mls ip multicast non-rpf-netflow (interface configuration mode)
show mls ip multicast

mls ip multicast non-rpf-netflow (interface configuration mode)

To enable the NetFlow-based non-RPF feature on a specific interface, use the **mls ip multicast non-rpf-netflow** command. Use the **no** form of this command to disable the feature.

mls ip multicast non-rpf-netflow

no mls ip multicast non-rpf-netflow

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

An RPF interface is used if a unicast packet is sent back to the source.

If a multicast packet encounters an RPF MFD shortcut, it is not sent to the route processor on the MSFC. The router processor never sees a copy of the packet forwarded by the hardware. The RPF MFDs are installed to switch packets arriving on the RPF interface.

A non-RPF MFD is an MFD that is installed to switch packets on the non-RPF VLAN. With RPF MFDs, the packets arriving on the RPF VLAN are forwarded to the outgoing VLANs. With non-RPF MFDs, the packets are bridged only on the VLAN on which it was received. The packet is not sent to the MSFC.

Examples

This example shows how to enable the NetFlow-based non-RPF feature:

```
Router(config-if)# mls ip multicast non-rpf-netflow
Router(config-if)#
```

Related Commands

mls ip multicast non-rpf-netflow (global configuration mode)
show mls ip multicast

mls ip multicast stub

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

mls ip multicast stub

no mls ip stub

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

When you enable the ACL-based method of filtering RPF failures by entering the **mls ip multicast stub** command on the redundant router, the following ACLs automatically download to the PFC and are applied to the interface you specify:

- access-list 100 permit ip A.B.C.0 0.0.0.255 any
- access-list 100 permit ip A.B.D.0 0.0.0.255 any
- access-list 100 permit ip any 224.0.0.0 0.0.0.255
- access-list 100 permit ip any 224.0.1.0 0.0.0.255
- access-list 100 deny ip any 224.0.0.0 15.255.255.255

The ACLs filter RPF failures and drop them in hardware so that they are not forwarded to the router.

Use the ACL-based method of filtering RPF failures only in sparse-mode stub networks where there are no downstream routers. For dense-mode groups, RPF failure packets have to be seen on the router for the PIM assert mechanism to function properly. Use CEF-or NetFlow-based rate limiting to rate limit RPF failures in dense-mode networks and sparse-mode transit networks.

Examples

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

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

Related Commands

show mls ip multicast

mls ip multicast threshold

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

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.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

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

This command does not affect already installed routes. For example, if you enter this command and shortcuts are already installed, the shortcuts will not be 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

mls rp ip (global configuration mode)
show mls ip multicast

mls ip pbr

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

mls ip pbr [**null0**]

no mls ip pbr

Syntax Description

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

Defaults

MLS support for policy-routed packets is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(12c)E1	This command was introduced on the Cisco 7600 series routers.
12.1(22)E3	This command was changed to support the **null0** keyword.

Usage Guidelines

The **mls ip pbr** command is supported on switches configured with a Supervisor Engine 1 only. On switches configured with a Supervisor Engine 2, PBR is performed in hardware by default.

When you enable hardware policy routing by entering the **mls ip pbr** command, all policy routing occurs in 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 MLS support for policy-routed packets:

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

mls ipx (interface configuration mode)

To enable MLS IPX on the interface, use the **mls ipx** command. Use the **no** form of this command to disable IPX on the interface.

mls ipx

no mls ipx

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to enable MLS IPX on an interface:

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

Related Commands

mls rp ipx (interface configuration mode)
show mls ipx

mls nde flow

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

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 exporting 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 maskbit*	Specifies a destination IP address and mask bits 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 mask bits to filter.
src-port *port-num*	Specifies the source port to filter.

Defaults

The defaults are as follows:

- All expired flows are exported until the filter is specified explicitly.
- Interface export is disabled (**no mls nde interface**).

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

The **mls nde flow** command adds filtering to the NDE. 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 NDE is disabled.

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 NDE is disabled.

Use the long subnet address format when specifying the **source** *ip-addr ip-mask*; for example, **source** 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.

Examples

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

```
Router(config)# mls nde flow include dest-port 35
Router(config)#
```

Related Commands

show mls netflow

mls nde interface

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

mls nde interface

no mls nde interface

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(13)E	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

With Release 12.1(13)E and later releases, 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 *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to populate 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

mls netflow
mls netflow sampling

mls nde sender

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

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

no mls nde sender

Syntax Description

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

Defaults

The defaults are as follows:

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(13)E	This command was changed to support NDE version 5.

Usage Guidelines

If you do not enter a *version*, the default *version* is **7**.

NDE on the PFC supports the following NDE versions to export the statistics captured on the PFC for Layer 3-switched traffic:

- Supervisor Engine 1 and PFC support NDE version 7
- Supervisor Engine 2 and PFC2 support these versions:
  - NDE versions 5 and 7 with Release 12.1(13)E and later releases
  - NDE version 7 only for releases prior to Release 12.1(13)E

NDE version 7 is supported on Cisco 7600 series routers configured with a Supervisor Engine 2 only.

Examples

This example shows how to enable the MLS NDE export feature:

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

This example shows how to disable the MLS NDE export feature:

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

Related Commands

show mls nde

mls nde src_address

To specify the source IP address used by the switch processor to send NDE packets to the Netflow Collector, use the **mls nde src_address** command. Use the **no** form of this command to remove a prior entry.

mls nde src_address *ip-addr* [**version** *version*]

no mls nde src_address *ip-addr*

Syntax Description

ip-addr	Source IP address of the NDE collector.
version *version*	(Optional) Keyword and variable to specify the NDE version; valid value is **7**.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(11b)E	This command was deprecated.

Usage Guidelines

When entering the *ip-addr*, the following guidelines must be used:

- The NDE source IP address you configure must be an unused address from the subnet of a router interface, and cannot be an address currently used by the interface.
- You cannot use an address from a subnet on a loopback interface.

When entering the *version*, the valid values are 7 and 8, but only version 7 is supported.

Examples

This example shows how to designate the source IP address of an NDE collector:

```
Router(config)# mls nde src_address 172.20.52.29
Router(config)#
```

Related Commands

show mls netflow

mls netflow

To enable the ability to create MLS NetFlow entries, use the **mls netflow** command. Use the **no** form of this command to disable the feature.

mls netflow

no mls netflow

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

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** global configuration command.

Examples

This example shows how to enable the ability to create MLS NetFlow entries:

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

This example shows how to disable the ability to create MLS NetFlow entries:

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

Related Commands

show mls netflow

mls netflow maximum-flows

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

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

no mls netflow maximum-flows

Syntax Description

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

Defaults

128

Command Modes

Global configuration

Command History

Release	Modification
12.1(23)E	Support for this command was introduced on the the Supervisor Engine 2.

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 settings:

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

Related Commands

show mls netflow table-contention

mls netflow sampling

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

mls netflow sampling

no mls netflow sampling

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(13)E	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

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

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

Sampled NetFlow is supported on systems configured with a Supervisor Engine 2 and on Layer 3 interfaces only.

Examples

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

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

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

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

Related Commands

mls sampling
show mls sampling

mls netflow usage notify

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

mls netflow usage notify {*threshold interval*}

no mls netflow usage notify

Syntax Description

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

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(23)E	Support for this command was introduced on the Supervisor Engine 2.

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 Cisco 7600 series router 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 and DFCs:

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

Related Commands

show mls netflow usage

mls qos (global configuration mode)

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

mls qos

no mls qos

Syntax Description

Defaults

QoS is globally disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(13)E	This command was changed to support the **queueing-only** option.

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

The **no mls qos queueing-only** command is equivalent to the **no mls qos** command.

In the **mls qos queueing-only** mode, all ports are put in a trust-cos mode. The configured (using the **mls qos trust** command) per-port trust mode is ignored.

Examples

This example shows how to enable QoS globally on the Cisco 7600 series router:

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

This example shows how to disable PFC QoS and enable port queueing globally on the Cisco 7600 series router:

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

This example shows how to disable QoS globally on the Cisco 7600 series router:

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

This example shows how to disable QoS and disable port-queueing mode globally on the Cisco 7600 series router:

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

Related Commands

mls qos (interface configuration mode)
show mls qos

mls qos (interface configuration mode)

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

mls qos

no mls qos

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(20)E	This command was deprecated.

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.

Examples

This example shows how to enable QoS on an interface:

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

Related Commands

show mls qos
mls qos (global configuration mode)

mls qos aggregate-policer

To define a named aggregate policer for use in policy maps, use the **mls qos aggregate-policer** command in global configuration mode. To delete a named aggregate policer, use the **no** form of this command.

mls qos aggregate-policer *name rate-bps* [*normal-burst-bytes* [*maximum-burst-bytes* | **pir** *peak-rate-bps* | *action-type action*]]

no mls qos aggregate-policer *name*

Syntax Description

name	Name of the aggregate policer. See the "Usage Guidelines" section for naming conventions.
rate-bps	Maximum bits per second. Range is 32000 to 10000000000.
normal-burst-bytes	(Optional) Normal burst bytes. Range is 1000 to 31250000.
maximum-burst-bytes	(Optional) Maximum burst bytes. Range is 1000 to 31250000 (if entered, this value must be set equal to normal-burst-bytes).
pir *peak-rate-bps*	(Optional) Keyword and argument that set the peak information rate (PIR). Range is 32000 to 10000000000. Default is equal to the normal (**cir**) rate.

action-type action	(Optional) Action type keyword. This command may include multiple action types and corresponding actions to set several actions simultaneously. Valid values are: • **conform-action**—Keyword that specifies the action to be taken when the rate is not exceeded. Valid actions are: – **drop**—Drops the packet. – **set-dscp-transmit** *value*—Sets the DSCP value and sends the packet. Valid entries are: 0 to 63 (differentiated code point value), af11 to af43 (match packets with specified AF DSCP), cs1 to cs7 (match packets with specified CS DSCP), default, or ef (match packets with the EF DSCP). – **set-mpls-exp-imposition-transmit** *number*—Sets experimental (exp) bits at the tag imposition. Valid range is 0 to 7. – **set-prec-transmit**—Rewrites packet precedence and sends the packet. – **transmit**—Transmits the packet. This is the default. • **exceed-action**—Keyword that specifies the action to be taken when QoS values are exceeded. Valid actions are: – **drop**—Drops the packet. This is the default. – **policed-dscp-transmit**—Changes the DSCP value according to the policed-dscp map and sends the packet. – **transmit**—Transmits the packet. • **violate-action**—Keyword that specifies the action to be taken when QoS values are violated. Valid actions are: – **drop**—Drops the packet. – **policed-dscp-transmit**—Changes the DSCP value according to the policed-dscp map and sends the packet. – **transmit**—Transmits the packet.

Defaults

The defaults are as follows:

- **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

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB.
12.3	This command was implemented on the Cisco 6500 and Cisco 7600.

Usage Guidelines

This policer can be shared by different policy map classes and on different interfaces. The Cisco 7600 series router 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 10 Gbps (entered as 32000 and 10000000000) and the range for the burst size is 1 KB (entered as 1000) to 31.25 MB (entered as 31250000). Modifying an existing aggregate rate limit entry causes that entry to be modified in NVRAM and in the Cisco 7600 series router if that entry is currently being used.

Note Because of 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 as well as in the Cisco 7600 series router 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**.

Aggregate policing works independently on each DFC-equipped switching module and independently on the PFC2, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module, PFC2, and any non-DFC-equipped switching modules that are supported by the PFC2 by entering the **show mls qos aggregate policer** command.

Examples

The following 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, to set DSCP to 48 when these rates are not exceeded, and to drop packets when these rates are exceeded:

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

Related Commands

Command	Description
policy (policy map)	Creates a per-interface policer and configures the policy-map class to use it.
set ip dscp (policy-map configuration)	Marks a packet by setting the IP DSCP in the ToS byte.
show mls qos aggregate policer	Displays information about the aggregate policer for MLS QoS.

mls qos bridged

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

mls qos bridged

no mls qos bridged

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

This command is not supported on OSM interfaces.

Examples

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

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

Related Commands

show mls qos

mls qos channel-consistency

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

mls qos channel-consistency

no mls qos channel-consistency

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)E1	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

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

In Release 12.1(12c)E1, you can enter the **mls qos channel-consistency** command to remove the following restriction:

With QoS disabled, an EtherChannel can contain interfaces with both strict-priority queues and interfaces without strict-priority queues. With QoS enabled, an EtherChannel cannot contain both interface types. If you enable QoS, interfaces drop out of any EtherChannels that contain both interface types.

Examples

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

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

This example shows how to disable QoS port attribute checks on 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. Use the **no** form of this command to remove a prior entry.

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.

Defaults

The defaults are as follows:

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

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

CoS values are configurable on physical LAN ports only.

This command is not supported on any WAN interface on the OSMs.

This command is not supported on 4-port Gigabit Ethernet WAN ports.

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

show mls qos

mls qos flow-policing

To enable QoS microflow policing, use the **mls qos flow-policing** command. Use the **no** form of this command to remove a prior entry.

mls qos flow-policing

no mls qos flow-policing

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(20)E	This command was deprecated.

Examples

This example shows how to enable QoS microflow policing:

```
Router(config)# mls qos flow-policing
Router(config)#
```

Related Commands

mls flow
show mls qos

mls qos map cos-dscp

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

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.

Defaults

The default CoS-to-DSCP configuration is listed in Table 2-15.

Table 2-15 CoS-to-DSCP Default Mapping

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

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 Cisco 7600 series router has one map.

Examples

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

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

Related Commands

mls qos map dscp-cos
mls qos map ip-prec-dscp
mls qos map policed-dscp
show mls qos

mls qos map dscp-cos

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

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.

Defaults

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

Table 2-16 DSCP-to-CoS Default Mapping

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

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 Cisco 7600 series router 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 mapping for trusted interfaces:

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

Related Commands

mls qos map cos-dscp
show mls qos

mls qos map ip-prec-dscp

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

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.

Defaults

The default IP precedence-to-DSCP configuration is listed in Table 2-17.

Table 2-17 IP Precedence-to-DSCP Default Mapping

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

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 Cisco 7600 series router 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-map 20 30 1 43 63 12 13 8
Router(config)#
```

Related Commands

mls qos map cos-dscp
mls qos map dscp-cos
mls qos map policed-dscp
show mls qos

mls qos map policed-dscp

To set the mapping of policed DSCP values to marked-down DSCP values, use the **mls qos map policed-dscp** command. Use the **no** form of this command to remove a prior entry.

mls qos map policed-dscp *dscp-list* **to** *policed-dscp*

no mls qos map policed-dscp

Syntax Description

dscp-list	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.

Defaults

No marked-down values are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

The DSCP-to-policed-DSCP map determines the marked-down DSCP value applied to out-of-profile flows. The Cisco 7600 series router 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 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 20 25 43 to 4
Router(config)#
```

Related Commands

mls qos map cos-dscp
mls qos map dscp-cos
mls qos map ip-prec-dscp
show mls qos

mls qos queueing-only

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

mls qos queueing-only

no mls qos [**queueing-only**]

Syntax Description

Defaults

QoS is globally disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)E	Support for this command was introduced on the Cisco 7600 series routers.

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 port-queueing mode globally:

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

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

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

Related Commands

mls qos (global configuration mode)
show mls qos

mls qos statistics-export (global configuration mode)

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

mls qos statistics-export

no mls qos statistics-export

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

You must enable data export globally to set up data export on your Cisco 7600 series router.

QoS statistics data export is not supported on OSM interfaces.

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

Examples

This example shows how to enable data export:

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

This example shows how to disable data export:

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

Related Commands

show mls qos statistics-export info

mls qos statistics-export (interface configuration mode)

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

mls qos statistics-export

no mls qos statistics-export

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

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 Cisco 7600 series router.

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

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 port export type)
- 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 statistics data export 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 data export:

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

This example shows how to disable data export:

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

Related Commands

mls qos statistics-export delimiter
show mls qos statistics-export info

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. Use the **no** form of this command to disable QoS statistics data export on the named aggregate policer.

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.

Defaults

Disabled for all shared aggregate policers

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

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 Cisco 7600 series router.

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, if you have the following configuration:

- Statistics data export enabled on the shared aggregate policer named “aggr_1”
- An EARL in the supervisor engine installed in slot 1
- An EARL on the DFC installed in slot 3

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

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

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

mls qos statistics-export delimiter
show mls qos statistics-export info

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. Use the **no** form of this command to disable QoS statistics data export for a class map.

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.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

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 Cisco 7600 series router.

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, statistics data per policer per interface is exported. If the interface is a physical interface, the following information is exported:

- Type (4 denotes 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 counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

If the interface is a Cisco 7600 series router 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 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:

- Statistics data export enabled on the class map named “class_1”
- An EARL in the supervisor engine installed in slot 1
- An EARL on the DFC installed in slot 3
- The system 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|
|6|class_1|in|1|24|32123|1475|1900|982361894|
|6|class_1|in|3|24|34265|6545|9845|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

mls qos statistics-export delimiter
show mls qos statistics-export info

mls qos statistics-export delimiter

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

mls qos statistics-export delimiter

no mls qos statistics-export delimiter

Syntax Description

This command has no arguments or keywords.

Defaults

The default delimiter is the pipe character (|).

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

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 Cisco 7600 series router.

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

show mls qos statistics-export info

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. Use the **no** form of this command to clear the configured values.

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

Syntax Description

host-name	Host name.
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; valid values are **kern**, **user**, **mail**, **daemon**, **auth**, **lpr**, **news**, **uucp**, **cron**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, and **local7**.
severity *severity-value*	(Optional) Specifies the severity level to export; valid values are **emerg**, **alert**, **crit**, **err**, **warning**, **notice**, **info**, and **debug**.

Defaults

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

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.
12.1(19)E	This command was changed to allow you to enter the full keyword for the facility and severity options.

Usage Guidelines

QoS statistics data export is not supported on OSM interfaces.

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

show mls qos statistics-export info

mls qos statistics-export interval

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

mls qos statistics-export interval *interval*

no mls qos statistics-export interval

Syntax Description

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

Defaults

300 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

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. Because exporting QoS statistics imposes a noticeable load on the Cisco 7600 series router, be careful when decreasing the interval.

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

show mls qos statistics-export info

mls qos trust

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

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.

Defaults

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
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.
12.1(11b)E	This command was changed to support OSMs.
12.1(13)E13	This command was changed to support these modules: • WS-X6148-RJ-45 • WS-X6148-RJ-45V • WS-X6148-RJ-21 • WS-X6148-RJ-21V

Usage Guidelines

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

You cannot configure the trust state on FlexWAN modules.

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

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

mls qos bridged
mls qos cos
mls qos vlan-based
show queueing interface

mls qos trust extend

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

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

no mls qos trust extend

Syntax Description

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

Defaults

The default settings are as follow:

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

Command Modes

Interface configuration

Command History

Release	Modification
12.1(13)E	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

If you set the phone to trusted mode, all the packets from the PC are sent untouched directly through the phone to the Cisco 7600 series router. 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 Cisco 7600 series router.

Each time 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 attached to the switch port in the 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 show queueing interface

mls qos vlan-based

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

mls qos vlan-based

no mls qos vlan-based

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

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

Per-VLAN QoS can be configured 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

mls qos bridged
mls qos cos
show queueing interface

mls rp ip (global configuration mode)

To enable external systems to establish IP shortcuts to the MSFC, use the **mls rp ip** command. Use the **no** form of this command to remove a prior entry.

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.

Defaults

No shortcuts are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to allow external systems to establish IP shortcuts with IP input access lists:

```
Router(config)# mls rp ip input-acl
Router(config)#
```

Related Commands

mls ip
show mls ip multicast

mls rp ip (interface configuration mode)

To enable external systems to enable MLS IP on a specified interface, use the **mls rp ip** command. Use the **no** form of this command to disable MLS IP.

mls rp ip

no mls rp ip

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to enable external systems to enable MLS IP on an interface:

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

Related Commands

mls rp ip (global configuration mode)
show mls ip multicast

mls rp ipx (global configuration mode)

To allow external systems to enable MLS IPX to the MSFC, use the **mls rp ipx** command. Use the **no** form of this command to remove a prior entry.

mls rp ipx [**input-acl**]

no mls rp ipx

Syntax Description

input-acl	(Optional) Enables MLS IPX and overrides ACLs.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to allow external systems to enable MLS IPX to the MSFC and override ACLs:

```
Router(config)# mls rp ipx input-acl
Router(config)#
```

Related Commands

mls rp ipx (interface configuration mode)
show mls rp ipx (refer to the *Cisco IOS Release 12.1 Command Reference*)

mls rp ipx (interface configuration mode)

To enable MLS IPX on the interface, use the **mls rp ipx** command to allow external systems. Use the **no** form of this command to disable MLS IPX on the interface.

mls rp ipx

no mls rp ipx

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to allow external systems to enable MLS IPX on an interface:

```
Router(config-if)# mls rp ipx
Router(config-if)#
```

Related Commands

mls rp ipx (global configuration mode)
show mls rp ipx (refer to the *Cisco IOS Release 12.1 Command Reference*)

mls rp management-interface

To enable the interface as a management interface, use the **mls rp management-interface** command. Use the **no** form of this command to remove a prior entry.

mls rp management-interface

no mls rp management-interface

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

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

show mls rp (refer to the *Cisco IOS Release 12.1 Command Reference*)

mls rp nde-address

To specify the NDE address, use the **mls rp nde-address** command. Use the **no** form of this command to remove a prior entry.

mls rp nde-address *ip-address*

no mls rp nde-address *ip-address*

Syntax Description

ip-address	NDE IP address.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

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

show mls rp (refer to the *Cisco IOS Release 12.1 Command Reference*)

mls rp vlan-id

To assign a VLAN ID to the interface, use the **mls rp vlan-id** command. Use the **no** form of this command to remove a prior entry.

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.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.
12.1(11b)EX	This command was changed to support extended-range VLANs.

Usage Guidelines

If your system is configured with a Supervisor Engine 1, valid values for *vlan-id* are from 1 to 1005. If your system is configured with a Supervisor Engine 2, valid values for *vlan-id* are from 1 to 4094. Extended-range VLANs are not supported on systems configured with a Supervisor Engine 1.

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

show mls rp (refer to the *Cisco IOS Release 12.1 Command Reference*)

mls rp vtp-domain

To link the interface to a VTP domain, use the **mls rp vtp-domain** command. Use the **no** form of this command to remove a prior entry.

mls rp vtp-domain *name*

no mls rp vtp-domain *name*

Syntax Description

name	VLAN domain name.

Defaults

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.

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

show mls rp (refer to the *Cisco IOS Release 12.1 Command Reference*)
vtp

mls sampling

To enable sampled NetFlow and specify the sampling method, use the **mls sampling** command. Use the **no** form of this command to disable sampled NetFlow.

mls sampling {{**time-based** *rate*} | {**packet-based** *rate* [*interval*]}}

no mls sampling

Syntax Description

time-based *rate*	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*	Packet-based sampling rate; valid values are **64**, **128**, **256**, **512**, **1024**, **2046**, **4096**, and **8192**.
interval	Sampling interval; valid values are from 4000 to 16000 milliseconds.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(13)E	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

Sampled NetFlow is supported on systems configured with a Supervisor Engine 2 and on Layer 3 interfaces only.

You can enable sampled NetFlow even if NDE is disabled, but no flows will be exported.

With packet-based sampling, a flow with a packet count of N is sampled N/M times, where M is the sampling rate.

Time-based sampling is based on a preset interval for each sampling rate. Table 2-18 lists the sample intervals for each rate and period.

Table 2-18 Time-based Sampling Intervals

Sampling Rate	Sampling Interval (milliseconds)	Sampling Period
64	64	4096
128	32	4096
256	16	4096
512	8	4096

Table 2-18 Time-based Sampling Intervals (continued)

Sampling Rate	Sampling Interval (milliseconds)	Sampling Period
1024	4	4096
2048	4	8192
4096	4	16384
8192	4	32768

Examples

This example shows how to enable time-based NetFlow sampling and set the sampling rate:

```
Router(config)# mls sampling time-based 1024
Router(config)#
```

This example shows how to enable packet-based NetFlow sampling and set the sampling rate and interval:

```
Router(config)# mls sampling packet-based 1024 4096
Router(config)#
```

Related Commands

mls netflow sampling
show mls sampling

mode

To set the redundancy mode, use the **mode** command.

mode {**rpr** | **rpr-plus**}

Syntax Description

rpr	Specifies RPR mode.
rpr-plus	Specifies RPR+ mode.

Defaults

The defaults are as follows:

- RPR+ mode if the active and standby supervisor engine have the same image
- RPR mode if different versions are installed

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(11b)EX	Support for this command was introduced on the Cisco 7600 series routers.
12.1(13)E	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

Enter the **redundancy** command in global configuration mode to enter the redundancy configuration mode. You can enter the **mode** command within the redundancy configuration mode.

Follow these guidelines when configuring your system to RPR+ mode:

- You must install compatible images on the active and standby supervisor engines to support the RPR+ mode.
- Both supervisor engines must run the same Cisco IOS software version.
- Any modules that are not online at the time of a switchover will be reset and reloaded on a switchover.
- The FIB tables are cleared on a switchover. As a result, routed traffic is interrupted until route tables reconverge.

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 RPR+:

```
Router(config)# redundancy
Router(config-red)# mode rpr-plus
Router(config-red)#
```

Related Commands

redundancy
redundancy force-switchover
show redundancy
show running-config

monitor session

To start a new SPAN or RSPAN session, add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, filter SPAN or RSPAN traffic to specific VLANs, or delete a SPAN or RSPAN session, use the **monitor session** command. Use the **no** form of this command to remove one or more source or destination interfaces from the SPAN or RSPAN session, remove a source VLAN from the SPAN or RSPAN session, or delete a SPAN or RSPAN session.

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*

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	SPAN source.
interface *type*	Interface type; see the "Usage Guidelines" section for formatting information.
vlan *vlan-id*	VLAN ID; valid values are from 1 to 4094.
rx	(Optional) Monitor-received traffic only.
tx	(Optional) Monitor-transmitted traffic only.
both	(Optional) Monitor-received and monitor-transmitted traffic.
remote vlan *rspan-vlan-id*	Specifies RSPAN VLAN as destination VLANs.
analysis-module *slot-number*	Network analysis module number; see the "Usage Guidelines" section for additional information.
data-port *port-number*	Data-port number; see the "Usage Guidelines" section for additional information.
destination	SPAN destination interface.
vlan *vlan-id*	VLAN ID; valid values are from 1 to 4094. See the "Usage Guidelines" section for formatting information.
filter vlan *vlan-range*	Limits SPAN source traffic to specific VLANs.
range *session-range*	Range of sessions.
local	Local session.

remote	Remote session.
all	All sessions.

Defaults

both

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(11b)E	This command was changed to include the **pos**, **atm**, and **ge-wan** keywords.
12.1(11b)E	This command was changed to support SPAN on DFC-equipped modules.
12.1(11b)EX	The command was changed to support extended-range VLANs.
12.1(13)E	This command was changed to support RSPAN.

Usage Guidelines

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 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, *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* options are supported on Network Analysis modules only.

The number of valid values for **port-channel** *number* depends on the software release. For releases prior to Release 12.1(3a)E3, valid values are from 1 to 256; for Releases 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Release 12.1(5c)EX and later support a maximum of 64 values ranging from 1 to 256. Release 12.1(13)E and later support a maximum of 64 values ranging from 1 to 282; values 257 to 282 are supported on the CSM and FWSM only.

If your system is configured with a Supervisor Engine 1, valid values for *vlan-id* are from 1 to 1005. If your system is configured with a Supervisor Engine 2, valid values for *vlan-id* are from 1 to 4094. Extended-range VLANs are not supported on systems configured with a Supervisor Engine 1.

You cannot share 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.

You can configure up to 64 SPAN destination interfaces but you can have one egress SPAN source interface and up to 64 ingress source interfaces only.

A particular SPAN session can either monitor VLANs or monitor individual interfaces—you cannot have a SPAN session that monitors both specific interfaces and specific VLANs. If you first configure a SPAN session with a source interface, and then try to add a source VLAN to the same SPAN session, you will get an error. You will 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.

Port channel interfaces display in the list of **interface** options if you have them configured. VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session** *session* **source vlan** *vlan-id* command.

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)#
```

Related Commands

remote-span
show monitor session

mpls l2transport route

To enable routing of Layer 2 packets over MPLS, use the **mpls l2transport route** command. Use the **no** form of this command to disable routing over MPLS.

mpls l2transport route *destination vc-id* [{**vc-type** [**vlan** | **ether**]}]

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.
vc-type	(Optional) Type of virtual connection used to route the VLAN packets. See the "Usage Guidelines" section for additional information.
vlan	(Optional) Specifies VLAN-based EoMPLS forwarding.
ether	(Optional) Specifies port-based EoMPLS forwarding.

Defaults

VLAN-based EoMPLS forwarding (type 4)

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.
12.1(11b)EX	This command was changed to include the **vc-type** keyword and support for type 5 forwarding.
12.1(13)E	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

Cisco 7600 series routers equipped with a Supervisor Engine 2 must be equipped with either an OSM or a FlexWAN port adapter that is facing the MPLS network and have a Layer-2 Ethernet port (non-OSM) facing the customer.

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 (**vlan**)—Allows all the traffic in a VLAN to use a single VC across the MPLS network.
- VC Type 5 (**ether**)—Allows all traffic on a port to share a single VC across the MPLS network.

An MPLS VLAN virtual circuit in Layer 2 runs across an MPLS cloud to connect VLAN interfaces on two PE routers.

Use the **mpls l2transport route** command on the VLAN interface of each PE router to route 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.

Routed virtual connections are supported on main interfaces, not subinterfaces.

The virtual-circuit ID must be unique to each virtual connection.

The **mpls l2transport route** command is not supported on systems configured with a Supervisor Engine 1.

Examples

This example shows how two routers, PE1 and PE2, establish a virtual connection to transport Layer 2 VLAN packets. PE1 has IP address 172.168.0.1. PE2 has IP address 192.16.0.1. The virtual connection ID is 50.

At PE1, you enter these commands:

```
PE1_router (config)# interface GigabitEthernet3/0
PE1_router(config-if) interface gigabitEthernet3/0.1
PE1_router(config-if)# mpls l2transport route 192.16.0.1 50
```

At PE2, you enter these commands:

```
PE2_router (config)# interface GigabitEthernet1/0
PE2_router(config-if) interface gigabitEthernet1/0.1
PE2_router(config-if)# mpls l2transport route 172.168.0.1 50
PE2_router(config-if)#
```

Related Commands

show mpls l2transport vc

mpls load-balance per-label

To enable the load balancing for tag-to-tag traffic, use the **mpls load-balance per-label** command. Use the **no** form of this command to return to the default settings.

mpls load-balance per-label

no mpls load-balance per-label

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)E	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

When it is enabled, 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 view the incoming label (indicated by an asterisk*) that is included in the load balancer.

Examples

This example shows how to enable load balancing for tag-to-tag traffic:

```
Router(config)# mpls load-balance per-label
Router(config)#
```

This example shows how to disable load balancing for tag-to-tag traffic:

```
Router(config)# no mpls load-balance per-label
Router(config)#s
```

Related Commands

show mpls ttfib

mtu

To adjust the maximum packet size or MTU size, use the **mtu** command. Use the **no** form of this command to return to the default settings.

mtu *bytes*

no mtu

Syntax Description

bytes	Byte size; valid values are from 64 to 9216 for SVI ports and from 1500 to 9216 for all other ports.

Defaults

Table 2-19 lists the default MTU values if jumbo frame support is disabled.

Table 2-19 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 jumbo frame support, the default is 64 for SVI ports and 9216 for all other ports. Jumbo frame support is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EX	Support for this command was introduced on the Cisco 7600 series routers.
12.1(11b)EX	This command was changed to support jumbo frames.
12.1(13)E	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

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 *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

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 specified with the **ip mtu** command are the same as the value 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

ip mtu (refer to the *Cisco IOS Release 12.1 Command Reference*)

name

To set the MST region name, use the **name** command. Use the **no** form of this command to return to the default name.

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.

Defaults

Empty string

Command Modes

MST configuration submode

Command History

Release	Modification
12.1(11b)EX	Support for this command was introduced on the Cisco 7600 series routers.
12.1(13)E	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

Two or more Cisco 7600 series routers 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 MST region name. A mistake would put the 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

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

net

To configure an IS-IS NET for the routing process, use the **net** command. Use the **no** form of this command to remove a NET.

net *net1* {**alt** *net2*}

no net *net*

Syntax Description

net1	NET NSAP name or address for the IS-IS routing process on the MSFC in the primary slot; see the "Usage Guidelines" section for additional information.
alt *net2*	NET name or address for the IS-IS routing process on the MSFC in the alternate slot; see the "Usage Guidelines" section for additional information.
net	NET NSAP name or address to be removed.

Defaults

The defaults are as follows:

- No NET is configured.
- IS-IS process is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

A NET is an NSAP where the last byte is always zero. A NET can be from 8 to 20 bytes. The last byte is always the n-selector and must be zero.

Under most circumstances, you should configure one and only one NET.

Even 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 system 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.

For IS-IS configuration information and examples, refer to the "Configuring Integrated IS-IS" chapter of the *Cisco IOS IP and IP Routing Configuration Guide*.

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 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

is-type (refer to the *Cisco IOS Release 12.1 Command Reference*)
router isis (refer to the *Cisco IOS Release 12.1 Command Reference*)

pagp learn-method

To learn the input interface of incoming packets, use the **pagp learn-method** command. Use the **no** form of this command to return to the default settings.

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.

Defaults

aggregation-port method

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

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

pagp learn-method
show pagp

pagp port-priority

To select a port in hot standby mode, use the **pagp port-priority** command. Use the **no** form of this command to return to the default settings.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

priority	Priority number; valid values are from 1 to 255.

Defaults

priority is **128**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

The higher the priority, the better the chances are that the port will be selected in the hot standby mode.

Examples

This example shows how to set the port priority:

```
Router(config-if)# pagp port-priority 45
Router(config-if)#
```

Related Commands

pagp learn-method
show pagp