clear mac address-table

To remove a specified address (or set of addresses) from the MAC address table, use the **clear mac address-table** command in privileged EXEC mode.

clear mac address-table [**dynamic** | **restricted static** | **permanent**] [**address** *mac-address*] [**interface** *type module port*]

clear mac address-table notification mac-move counter [*vlan*]

Clearing a Dynamic Address Using a Supervisor 720

clear mac address-table dynamic [**address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id*]

Clearing a Dynamic Address Using a Supervisor Engine 2

clear mac address-table dynamic [**address** *mac-address* | **interface** *interface-type interface-number* | **protocol** {**assigned** | **ip** | **ipx** | **other** } [**vlan** *vlan-id*]

Syntax Description

dynamic	(Optional) Clears only dynamic addresses.
restricted static	(Optional) Clears only restricted static addresses.
permanent	(Optional) Clears only permanent addresses.
address	(Optional) Clears only a specified address.
mac-address	(Optional) Specifies the MAC address.
interface	(Optional) Clears all addresses for an interface.
type	(Optional) Interface type: ethernet, fastethernet, fddi, atm, or port channel.
slot	(Optional) Module interface number.
interface-type interface-number	(Optional) Module and port number. See the "Usage Guidelines" section for valid values.
notification mac-move counter	Clears the MAC-move notification counters.
vlan	(Optional) Specifies the VLAN to clear the MAC-move notification counters.
protocol assigned	(Optional) Specifies the assigned protocol accounts for such protocols such as DECnet, Banyan VINES, and AppleTalk.
protocol ip | **ipx**	(Optional) Specifies the protocol type of the entries to clear.
protocol other	(Optional) Specifies the protocol types (other than IP or IPX) of the entries to clear.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

module	(Optional) The module interface number: • 0 for fixed • 1 or A for module A • 2 or B for module B
port	(Optional) Port interface number ranging from 1 to 28: • 1 to 25 for Ethernet (fixed) • 26, 27 for Fast Ethernet (fixed) • Port channel

Command Default

The dynamic addresses are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

If the **clear mac address-table** command is invoked with no options, all dynamic addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all interfaces. If you specify an interface but do not specify an address, all addresses on the specified interface are removed.

If a targeted address is not present in the MAC forwarding table, the following error message appears:

```
MAC address not found
```

Clearing a Dynamic Address

Enter the **clear mac address-table dynamic** command to remove all dynamic entries from the table.

The following values are valid for *interface-type*:

- fastethernet
- gigabitethernet
- port-channel

Setting the Module and Port

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

Examples

The following example shows how to clear all dynamic addresses in the MAC forwarding table:

```
Router# clear mac address-table dynamic
```

The following example shows how to clear the MAC-move notification counters on a specific VLAN:

```
Router# clear mac address-table notification mac-move counter 202
```

The following example shows the permanent address 0040.C80A.2F07 being cleared on Ethernet port 1:

```
Router# clear mac address-table permanent address 0040.C80A.2F07 interface ethernet 0/1
```

Related Commands

Command	Description
mac address-table aging-time	Configures the length of time the switch keeps dynamic MAC addresses in memory before discarding.
mac address-table permanent	Associates a permanent unicast or multicast MAC address with a particular switched port interface.
mac address-table restricted static	Associates a restricted static address with a particular switched port interface.
mac address-table secure	Associates a secure static address with a particular switched port interface.
mac address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
show mac address-table	Displays addresses in the MAC address table for a switched port or module.
show mac address-table secure	Displays the addressing security configuration.
show mac address-table security	Displays the addressing security configuration.

clear platform feature-manager

To clear platform-specific feature manager configuration commands, use the **clear platform feature-manager** command.

clear platform feature-manager {**consistency-check** | **exception** {**interface** {**async** *number* | **auto-template** *number* | **ctunnel** *number* | **dialer** *number* | **esconphy** *number* | **filter** *number* | **filtergroup** *number* | **gigabitethernet** *number* | **group-async** *number* | **longreachethernet** *number* | **loopback** *number* | **mfr** *number* | **multilink** *number* | **null** *number* | **port-channel** *number* | **portgroup** *number* | **pos-channel** *number* | **sysclock** *number* | **tengigabitethernet** *number* | **tunnel** *number* | **vif** *number* | **virtual-template** *number* | **virtual-tokenring** *number* | **vlan** *vlan_id* | **control-plane** *number* | **fcpa** *number* | **voabypassin** *number* | **voabypassout** *number* | **voafilterin** *number* | **voafilterout** *number* | **voain** *number* | **voaout** *number*}}}

Syntax Description

consistency-check	Specifies the consistency checker logs.
exception	Specifies the exception-state-related logs.
interface	Displays the available interfaces.
async *number*	Specifies the asynchronous interface number. Range is 1–999.
auto-template *number*	Specifies the auto-template interface number. Range is 1–999.
ctunnel *number*	Specifies the Ctunnel interface number. Range is 0–2147483647.
dialer *number*	Specifies the dialer interface number. Range is 0–255.
esconphy *number*	Specifies the esconPhy interface number. Range is 1–6.
filter *number*	Specifies the filter interface number. Range is 1–6.
filtergroup *number*	Specifies the filter group interface number. Range is 1–6.
gigabitethernet *number*	Specifies the gigabit Ethernet interface number. Range is 1–6.
longreachethernet *number*	Specifies the long-reach Ethernet interface number. Range is 1–6.
loopback *number*	Specifies the loopback interface number. Range is 1–2147483647.
mfr *number*	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink *number*	Specifies the multilink-group interface number. Range is 1–2147483647.
null *number*	Specifies the null interface number. Range is 0–0.
port-channel *number*	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup *number*	Specifies the portgroup interface number. Range is 1–6.
pos-channel *number*	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock *number*	Specifies the telecom-bus Clock Controller interface number. Range is 1–6.
tengigabitethernet *number*	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel *number*	Specifies the tunnel interface number. Range is 1–2147483647.
vif *number*	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template *number*	Specifies the virtual template interface number. Range is 1–200.

virtual-tokenring *number*	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan *vlan_id*	Specifies the VLAN interface number. Range is 1–4094.
fcpa *number*	Specifies the fibre channel interface number. Range is 1–6.
control-plane *number*	Specifies the control plane interface number. Range is 1–6.
voabypassin *number*	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout *number*	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin *number*	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout *number*	Specifies the VOA filter-out interface number. Range is 1–6.
voain *number*	Specifies the VOA in interface number. Range is 1–6.
voaout *number*	Specifies the VOA out interface number. Range is 1–6.
async *number*	Specifies the asynchronous interface number. Range is 1–999.

Defaults

None.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear the platform-specific feature manager configuration that has an asynchronous interface number of 4:

```
Router# clear platform feature-manager exception interface async 4
```

Related Commands

Command	Description
show platform software feature-manager	Displays platform software-specific feature manager configuration commands.

clear platform flow ip

This command clears the NetFlow hardware IP entries.

clear platform flow ip {**destination {hostname** {**instance | module**} **| IP address**} **| instance | module | source** {**hostname** {**instance | module**} **| IP address** }} {*number*}

Syntax Description

destination	This clears the entries with the destination address.
hostname	The destination IP address.
instance	It contains the earl instance.
module *number*	The module number ranges from 1-6.
IP Address	The destination IP address.
source	The source IP address.
instance *number*	This contains the earl instance which ranges from 0-0.
module *number*	The module number ranges from 1-6.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear the platform IP destination host name module 4:

```
Router(config)# clear platform flow ip destination hostname module 4
```

Related Commands

Command	Description
show platform flow ip	Displays the NetFlow hardware IP entries.

clear platform flow ipv6

To clear platform flow IPv6 by instance or module number, use the **clear platform flow ipv6** command.

clear platform flow ipv6 {**instance** *number* | **module** *number*}

Syntax Description

instance *number*	Specifies the EARL instance.
module *number*	Specifies the module number. Range is 1–6.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear platform flow IPv6 for module 4:

```
Router# clear platform flow ipv6 module 4
```

Related Commands

Command	Description
show platform flow ipv6	Displays the platform flow IPv6 by instance or module number.

clear platform hardware acl

To clear hardware ACL statistics, use the **clear platform hardware acl accounting** command.

clear platform hardware acl {**accounting-stats** {**module** *number*} | **hit-counts** {**all** {**module** *number*} | **compaction** {**ipv6** {**all** {**module**}} | **dest** {**module**} | **src** {**module**}} | **global_qos** {**all** {**module**} | **in** {**ip** {**module**} | **ipv6** {**module**} | **mac** {**module**} | **mpls** {**module**}} | **out** {**ip** {**module**} | **ipv6** {**module**} | **mac** {**module**} | **mpls** {**module**}}} | **interface** {**async** *number* | **auto-template** *number* | **ctunnel** *number* | **dialer** *number* | **esconphy** *number* | **filter** *number* | **filtergroup** *number* | **gigabitethernet** *number* | **longreachethernet** *number* | **loopback** *number* | **mfr** *number* | **multilink** *number* | **null** *number* | **port-channel** *number* | **portgroup** *number* | **pos-channel** *number* | **sysclock** *number* | **tengigabitethernet** *number* | **tunnel** *number* | **vif** *number* | **virtual-template** *number* | **virtual-tokenring** *number* | **vlan** *vlan_id* | **control-plane** *number* | **fcpa** *number* | **voabypassin** *number* | **voabypassout** *number* | **voafilterin** *number* | **voafilterout** *number* | **voain** *number* | **voaout** *number*}} | **rbacl** {**all** {**module** *number*} | **tcam** {**A** {**index** *number*} | **B** {**index** *number*}}}

Syntax Description

accounting-stats	Specifies accounting statistics.
module *number*	Specifies module number.
hit-counts	Specifies hit counts.
all	Specifies all entries.
compaction	Specifies compaction entries.
ipv6	Specifies IPv6 compaction entries.
dest	Specifies destination addresses.
src	Specifies source addresses.
global_qos	Specifies global-QoS entries.
in	Specifies inbound entries.
ip	Specifies the IP protocol.
mac	Specifies the MAC protocol.
mpls	Specifies the MPLS protocol.
out	Specifies outbound entries.
interface	Lists the various interfaces to choose ACL statistics for.
async *number*	Specifies the asynchronous interface number. Range is 1–999.
auto-template *number*	Specifies the auto-template interface number. Range is 1–999.
ctunnel *number*	Specifies the channel tunnel interface number. Range is 0–2147483647.
dialer *number*	Specifies the dialer interface number. Range is 0–255.
esconphy *number*	Specifies the EsconPhy interface number. Range is 1–6.
filter *number*	Specifies the filter interface number. Range is 1–6.
filtergroup *number*	Specifies the filter group interface number. Range is 1–6.
gigabitethernet *number*	Specifies the Gigabit Ethernet interface number. Range is 1–6.
longreachethernet *number*	Specifies the long-reach Ethernet interface number. Range is 1–6.

loopback *number*	Specifies the loopback interface number. Range is 1–2147483647.
mfr *number*	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink *number*	Specifies the multilink group interface number. Range is 1–2147483647.
null *number*	Specifies the null interface number. Range is 0–0.
port-channel *number*	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup *number*	Specifies the port group interface number. Range is 1–6.
pos-channel *number*	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock *number*	Specifies the telecom bus clock controller interface number. Range is 1–6.
tengigabitethernet *number*	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel *number*	Specifies the tunnel interface number. Range is 1–2147483647.
vif *number*	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template *number*	Specifies the virtual template interface number. Range is 1–200.
virtual-tokenring *number*	Specifies the virtual Token Ring interface number. Range is 1–2147483647.
vlan *vlan_id*	Specifies the VLAN interface number. Range is 1–4094.
fcpa *number*	Specifies the Fibre Channel interface number. Range is 1–6.
voabypassin *number*	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout *number*	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin *number*	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout *number*	Specifies the VOA filter-out interface number. Range is 1–6.
voain *number*	Specifies the VOA in interface number. Range is 1–6.
voaout *number*	Specifies the VOA out interface number. Range is 1–6.
rbacl	Displays RBACL entries.
tcam A, **tcam B**	Displays entries for TCAM A, TCAM B.
index *number*	Specifies the TCAM index number. Range is 0–131071.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear the hardware ACL accounting statistics for module 4:

```
Router# clear platform hardware acl accounting-stats module 4
```

Related Commands

Command	Description
platform hardware acl	Configures hardware ACL statistics.

clear platform hardware capacity rewrite-engine

To clear platform flow IPv6 by instance or module number, use the **clear platform flow ipv6** command.

clear platform flow ipv6 {**instance** *number* | **module** *number*}

Syntax Description

instance *number*	Specifies the EARL instance.
module *number*	Specifies the module number. Range is 1–6.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear platform flow IPv6 for module 4:

```
Router# clear platform flow ipv6 module 4
```

Related Commands

Command	Description
show platform flow ipv6	Displays the platform flow IPv6 by instance or module number.

clear platform hardware cef

To clear platform hardware CEF, use the **clear platform hardware cef** command.

clear platform hardware cef {**ip** {**accounting** {**per-prefix** {**A.B.C.D** | **all**}}} | **ipv6** {**accounting** {**per-prefix**}}}

Syntax Description

ip	Specifies the constant CEF IP.
accounting	Specifies the accounting statistics.
per-prefix	Specifies the per-prefix accounting statistics.
A.B.C.D	Specifies the prefix entry.
all	Specifies all of the per-prefix accounting statistics.
ipv6	Specifies the IPv6 CEF statistics.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear the hardware CEF IPv6 accounting prefix entry:

```
Router# clear platform hardware cef ipv6 accounting per-prefix 34
```

Related Commands

Command	Description
show platform hardware cef	Displays the platform hardware CEF entries.

clear platform hardware ehc

To clear platform hardware EHC information, use the **clear platform hardware ehc** command.

clear platform hardware ehc {**ids** | **rate-limiter** | **xcpt**}

SyntaxDescription

ids	Performs a hardware IDS check.
rate-limiter	Specifies the hardware rate limits.
xcpt	Specifies the hardware exceptions.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

This example shows how to clear the platform hardware EHC exceptions:

```
Router# clear platform hardware ehc xcpt
```

clear platform hardware statistics

To clear the platform hardware statistics information by module number, use the **clear platform hardware statistics** command.

clear platform hardware statistics {**module** *number*}

Syntax Description

module *number*	Specifies the module number. Range is 1–6.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear the platform hardware statistics for module 4:

```
Router# clear platform hardware statistics module 4
```

Related Commands

Command	Description
show platform hardware statistics	Displays the configuration for platform hardware statistics.

clear platform qos

To clear the multilayer switching (MLS) aggregate quality of service (QoS) statistics, use the **clear platform qos** command in privileged EXEC mode.

clear platform qos [**ip** | **mac** | **mpls** | **ipv6** | **arp** [*interface-type interface-number* | **null** *interface-number* | **port-channel** *number* | **vlan** *vlan-id*]]

Syntax Description

ip	(Optional) Clears MLS IP aggregate QoS statistics.
mac	(Optional) Clears MLS MAC aggregate QoS statistics.
mpls	(Optional) Clears MLS MPLS aggregate QoS statistics.
ipv6	(Optional) Clears MLS IPv6 aggregate QoS statistics.
arp	(Optional) Clears MLS ARP aggregate QoS statistics.
interface-type	(Optional) Interface type. Possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values.
interface-number	(Optional) Module and port number.See the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface. The valid value is 0.
port-channel *number*	(Optional) Specifies the channel interface. Valid values are a maximum of 64 values ranging from 1 to 256.
vlan *vlan-id*	(Optional) Specifies the VLAN ID. Valid values are from 1 to 4094.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

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

If you enter the **clear platform qos** command with no arguments, the global and per-interface aggregate QoS counters for all protocols are cleared.

If you do not enter an interface type, the protocol aggregate-QoS counters for all interfaces are cleared.

Note Entering the **clear platform qos** command affects the policing token bucket counters and might briefly allow traffic to be forwarded that would otherwise be policed.

Examples

This example shows how to clear the global and per-interface aggregate-QoS counters for all protocols:

```
Router# clear platform qos
```

This example shows how to clear the specific protocol aggregate-QoS counters for all interfaces:

```
Router# clear platform qos ip
```

Related Commands

Command	Description
show platform qos	Displays MLS QoS information.

clear platform software acl accounting-stats

To clear the platform software ACL accounting statistics information by module number, use the **clear platform sofware acl accounting-stats** command.

clear platform software acl accounting-stats {**module** *number*}

Syntax Description

module *number*	Specifies the module number. Range is 1–6.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear the platform software ACL accounting statistics for module 4:

```
Router# clear platform software acl accounting-stats module 4
```

Related Commands

Command	Description
show platform software acl accounting-stats	Displays the configuration for platform software ACL accounting statistics.

clear platform software met

To clear platform software MET-related statistics, use the **clear platform software met** command.

clear platform software met {**statistics**}

Syntax Description

statistics	Displays MET statistics information.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to clear platform software MET statistics:

```
Router# clear platform software met detail
```

Related Commands

Command	Description
platform software met	Configures the platform software MET-related information.

debug netdr

To debug NetDriver activity, use the **debug netdr** command. Use the **no** form of this command to disable debugging output.

debug netdr {**all** | **data** | **error**}

no debug netdr {**all** | **data** | **error**}

Syntax Description

all	Debugs all NetDriver activity.
data	Debugs NetDriver data flow.
error	Debugs NetDriver errors.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command was extended to 12.2SY.

Examples

This example shows how to debug the NetDriver data flow:

```
Router# debug netdr data
NetDriver Receive Data on interrupt debugging is on
NetDriver Receive Data debugging is on
NetDriver Transmit Data debugging is on
NetDriver Relay Data debugging is on
Router#
2d21h: const_ether_vlan_vencap() Vlan1:
2d21h:    src_vlan=0x1  src_indx=0x3  len=0xE9  bpdu=0
2d21h:    index_dir=0  dest_indx=0x0  dont_lrn=0
2d21h:    Dbus hdr:  00000000 00010000 00030000 E9000000
2d21h:               00000000 00000000 00000000 00000000
2d21h:    MAC hdr:  dmac=00801C.938040, smac=00503E.8D6400, typelen=0800
2d21h:    IP hdr:  45C000DB 02F30000 FF066331 AC143412 AB45C8CC
2d21h: fx1000_process_receive_packet() Vlan1:
2d21h:    src_vlan=0x1  src_indx=0x108  len=0x40  bpdu=0
2d21h:    index_dir=0  dest_indx=0x3  dont_lrn=0
2d21h:    Dbus hdr:  60000000 00010000 01080000 40100000
2d21h:               0006AC14 3412AB45 C8CC0000 00030000
2d21h:    MAC hdr:  dmac=00503E.8D6400, smac=00605C.865B28, typelen=0800
2d21h:    IP hdr:  45000028 B5254000 7D06F471 AB45C8CC AC143412
<... output truncated ...>
Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs NetDriver continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture

To debug NetDriver capture activity, use the **debug netdr capture** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture [**and-filter** [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

no debug netdr capture [**and-filter** [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

Syntax Description

and-filter	(Optional) Applies filters.
destination-ip-address	(Optional) Captures all packets matching a destination IP address.
ipaddr	Captures packets for a specific destination IP address.
ipv6 *ipaddr*	Captures all packets matching the IPv6 destination IP address.
dmac *mac-addr*	(Optional) Captures packets matching a destination MAC address index.
dstindex *index-value*	(Optional) Captures all packets matching a destination index; valid values are 0 to 1048575.
ethertype *ethertype*	(Optional) Captures all packets matching an ethertype; ethertype must be entered in hexidecimal format.
interface *interface*	(Optional) Captures packets related to the interface. See Usage Guidelines.
smac *smac*	(Optional) Captures packets matching the source MAC address; smac must be entered in hexidecimal format.
source-ip-address	(Optional) Captures all packets matching a source IP address.
srcindex *index-value*	(Optional) Captures all packets matching a source index; valid values are 0 to 1048575.
vlan *vlan-num*	(Optional) Captures packets matching the VLAN number; valid VLAN numbers are 0 to 4095.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

You can use the following interface types:

- Async
- Auto-template
- CTunnel
- Dialer
- EsconPhy
- Fcpa
- Filter
- Filtergroup
- GMPLS
- GigabitEthernet
- Group-Async
- LISP
- LongReachEthernet
- Looopback
- Lspvif
- MFR
- Multilink
- Null
- Port-channel
- Sysclock
- TenGigabitEthernet
- Tunnel
- Vif
- Virtual-Ethernet
- Virtual-Template
- Virtual-TokenRing
- VLAN
- VoaBypassIn
- VoaBypassOut
- VoaFilterIn
- VoaFilterOut
- VoaIn
- VoaOut

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr capture
```

```
Router#
```

Related Commands

Command	Description
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture and-filter

To debug NetDriver capture activity using an **and** function, use the **debug netdr capture and-filter** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture and-filter [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

no debug netdr capture and-filter [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

Syntax Description

destination-ip-address	(Optional) Captures all packets matching a destination IP address.
ipaddr	Captures packets for a specific destination IP address.
ipv6 *ipaddr*	Captures all packets matching the IPv6 destination IP address.
dmac *mac-addr*	(Optional) Captures packets matching a destination MAC address index.
dstindex *index-value*	(Optional) Captures all packets matching a destination index; valid values are 0 to 1048575.
ethertype *ethertype*	(Optional) Captures all packets matching an ethertype; ethertype must be entered in hexidecimal format.
interface *interface*	(Optional) Captures packets related to the interface. See Usage Guidelines.
smac *smac*	(Optional) Captures packets matching the source MAC address; smac must be entered in hexidecimal format.
source-ip-addr ess	(Optional) Captures all packets matching a source IP address.
srcindex *index-value*	(Optional) Captures all packets matching a source index; valid values are 0 to 1048575.
vlan *vlan-num*	(Optional) Captures packets matching the VLAN number; valid VLAN numbers are 0 to 4095.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

You can use the following interface types:

- Async
- Auto-template
- CTunnel
- Dialer
- EsconPhy
- Fcpa
- Filter
- Filtergroup
- GMPLS
- GigabitEthernet
- Group-Async
- LISP
- LongReachEthernet
- Looopback
- Lspvif
- MFR
- Multilink
- Null
- Port-channel
- Sysclock
- TenGigabitEthernet
- Tunnel
- Vif
- Virtual-Ethernet
- Virtual-Template
- Virtual-TokenRing
- VLAN
- VoaBypassIn
- VoaBypassOut
- VoaFilterIn
- VoaFilterOut
- VoaIn
- VoaOut

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr capture

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture continuous

To debug NetDriver capture activity continuously, use the **debug netdr capture continuous** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture continuous [**and-filter** | **destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **or-filter** [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*] | **rx** [**and-filter** | **destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dti-type** *value* | **dti-value** *value* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **or-filter** [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*] | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

no debug netdr capture continuous [**and-filter** | **destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **or-filter** [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*] | **rx** [**and-filter** | **destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dti-type** *value* | **dti-value** *value* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **or-filter** [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*] | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

Syntax Description

and-filter	(Optional) Applies filters.
destination-ip-address	(Optional) Captures all packets matching a destination IP address.
ipaddr	Captures packets for a specific destination IP address.
ipv6 *ipaddr*	Captures all packets matching the IPv6 destination IP address.
dmac *mac-addr*	(Optional) Captures packets matching a destination MAC address index.
dstindex *index-value*	(Optional) Captures all packets matching a destination index; valid values are 0 to 1048575.
ethertype *ethertype*	(Optional) Captures all packets matching an ethertype; ethertype must be entered in hexidecimal format.
interface *interface*	(Optional) Captures packets related to the interface. See Usage Guidelines.
or-filter	(Optional) Applies filters.
rx	(Optional) Captures incoming packets only.
dti-type *value*	(Optional) Captures all packets matching the 3-bit dti type; valid values are 0 to 7.
dti-value *value*	(Optional) Captures all packets matching the 21-bit dti value; valid values are 0 to 4096.
smac *smac*	(Optional) Captures packets matching the source MAC address; smac must be entered in hexidecimal format.

source-ip-address	(Optional) Captures all packets matching a source IP address.
srcindex *index-value*	(Optional) Captures all packets matching a source index; valid values are 0 to 1048575.
vlan *vlan-num*	(Optional) Captures packets matching the VLAN number; valid VLAN numbers are 0 to 4095.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

You can use the following interface types:

- Async
- Auto-template
- CTunnel
- Dialer
- EsconPhy
- Fcpa
- Filter
- Filtergroup
- GMPLS
- GigabitEthernet
- Group-Async
- LISP
- LongReachEthernet
- Looopback
- Lspvif
- MFR
- Multilink
- Null
- Port-channel
- Sysclock
- TenGigabitEthernet

- Tunnel
- Vif
- Virtual-Ethernet
- Virtual-Template
- Virtual-TokenRing
- VLAN
- VoaBypassIn
- VoaBypassOut
- VoaFilterIn
- VoaFilterOut
- VoaIn
- VoaOut

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr capture


Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture destination-ip-address

To debug NetDriver capture activity capturing all packets matching a destination IP address, use the **debug netdr capture destination-ip-address** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture destination-ip-address {*ipaddr* | **ipv6** *ipaddr*}

no debug netdr capture destination-ip-address {*ipaddr* | **ipv6** *ipaddr*}

Syntax Description

ipaddr	Captures packets for a specific destination IP address.
ipv6 *ipaddr*	Captures all packets matching the IPv6 destination IP address.

Defaults

None

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Command Modes

Privileged EXEC

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr capture


Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.

Command	Description
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture dmac

To debug NetDriver capture activity by capturing all matching destination MAC addresses, use the **debug netdr capture dmac** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture dmac [*mac-addr*]

no debug netdr capture dmac [*mac-addr*]

Syntax Description

mac-addr	(Optional) Captures packets matching a destination MAC address index.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr capture


Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.

Command	Description
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture dstindex

To debug NetDriver capture activity capturing all packets matching the destination index, use the **debug netdr capture dstindex** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture dstindex [*index-value*]

no debug netdr capture dstindex [*index-value*]

Syntax Description

index-value	(Optional) Captures all packets matching a destination index; valid values are 0 to 1048575.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr capture

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.

Command	Description
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture ethertype

To debug NetDriver capture ethertype activity, use the **debug netdr capture ethertype** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output. .

debug netdr capture ethertype [*ethertype*]

no debug netdr capture ethertype [*ethertype*]

Syntax Description

ethertype	(Optional) Captures all packets matching an ethertype; ethertype must be entered in hexidecimal format.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDriver ethertype:

```
Router# debug netdr capture ethertype

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.

Command	Description
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture interface

To debug NetDriver capture interface activity, use the **debug netdr capture interface** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture interface [*interface*]

no debug netdr capture interface [*interface*]

Syntax Description

interface	(Optional) Captures packets related to the interface. See Usage Guidelines.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

You can use the following interface types:

- Async
- Auto-template
- CTunnel
- Dialer
- EsconPhy
- Fcpa
- Filter
- Filtergroup
- GMPLS
- GigabitEthernet
- Group-Async
- LISP
- LongReachEthernet
- Looopback
- Lspvif
- MFR

- Multilink
- Null
- Port-channel
- Sysclock
- TenGigabitEthernet
- Tunnel
- Vif
- Virtual-Ethernet
- Virtual-Template
- Virtual-TokenRing
- VLAN
- VoaBypassIn
- VoaBypassOut
- VoaFilterIn
- VoaFilterOut
- VoaIn
- VoaOut

Examples

This example shows how to debug the NetDriver interface activity:

```
Router# debug netdr capture interface

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.

Command	Description
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture or-filter

To debug NetDriver capture activity using an **or** function, use the **debug netdr capture or-filter** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture or-filter [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

no debug netdr capture or-filter [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

Syntax Description

destination-ip-address	(Optional) Captures all packets matching a destination IP address.
ipaddr	Captures packets for a specific destination IP address.
ipv6 *ipaddr*	Captures all packets matching the IPv6 destination IP address.
dmac *mac-addr*	(Optional) Captures packets matching a destination MAC address index.
dstindex *index-value*	(Optional) Captures all packets matching a destination index; valid values are 0 to 1048575.
ethertype *ethertype*	(Optional) Captures all packets matching an ethertype; ethertype must be entered in hexidecimal format.
interface *interface*	(Optional) Captures packets related to the interface. See Usage Guidelines.
smac *smac*	(Optional) Captures packets matching the source MAC address; smac must be entered in hexidecimal format.
source-ip-address	(Optional) Captures all packets matching a source IP address.
srcindex *index-value*	(Optional) Captures all packets matching a source index; valid values are 0 to 1048575.
vlan *vlan-num*	(Optional) Captures packets matching the VLAN number; valid VLAN numbers are 0 to 4095.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

You can use the following interface types:

- Async
- Auto-template
- CTunnel
- Dialer
- EsconPhy
- Fcpa
- Filter
- Filtergroup
- GMPLS
- GigabitEthernet
- Group-Async
- LISP
- LongReachEthernet
- Looopback
- Lspvif
- MFR
- Multilink
- Null
- Port-channel
- Sysclock
- TenGigabitEthernet
- Tunnel
- Vif
- Virtual-Ethernet
- Virtual-Template
- Virtual-TokenRing
- VLAN
- VoaBypassIn
- VoaBypassOut
- VoaFilterIn
- VoaFilterOut
- VoaIn
- VoaOut

Examples

This example shows how to debug the NetDriver or-filter:

```
Router# debug netdr capture or-filter

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture rx

To debug NetDriver capture activity by capturing incoming packets only, use the **debug netdr capture rx** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture **rx** [**dti-type** *value* | **dti-value** *value*]

no debug netdr capture rx [**dti-type** *value* | **dti-value** *value*]

Syntax Description

dti-type *value*	(Optional) Captures all packets matching the 3-bit dti type; valid values are 0 to 7.
dti-value *value*	(Optional) Captures all packets matching the 21-bit dti value; valid values are 0 to 4096.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDrivers incoming packets:

```
Router# debug netdr capture rx


Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.

Command	Description
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture smac

To debug NetDriver capture activity by capturing matching source MAC addresses, use the **debug netdr capture smac** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture smac [*smac*]

no debug netdr capture smac [*smac*]

Syntax Description

smac	(Optional) Captures packets matching the source MAC address; smac must be entered in hexidecimal format.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDriver by capturing the source MAC addresses:

```
Router# debug netdr capture smac

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.

Command	Description
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture source-ip-address

To debug NetDriver capture activity by capturing all packets matching a source IP address, use the **debug netdr capture source-ip-address** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture source-ip-address {*ipaddr* | **ipv6** *ipaddr*}

no debug netdr capture source-ip-address {*ipaddr* | **ipv6** *ipaddr*}

Syntax Description

ipaddr	Captures packets for a specific destination IP address.
ipv6 *ipaddr*	Captures all packets matching the IPv6 destination IP address.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDriver: source IP address

```
Router# debug netdr capture source-ip-address

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.

Command	Description
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture srcindex

To debug NetDriver capture activity by capturing all packets matching the source index, use the **debug netdr capture srcindex** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture srcindex [*index-value***]**

no debug netdr capture srcindex [*index-value***]**

Syntax Description

index-value	(Optional) Captures all packets matching a source index; valid values are 0 to 1048575.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDriver by capturing all packets matching the source index:

```
Router# debug netdr capture srcindex

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.

Command	Description
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture tx

To debug NetDriver capture activity by capturing the outgoing packets only, use the **debug netdr capture tx** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture tx [**and-filter** | **destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **or-filter** [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

no debug netdr capture tx [**andand-filter** | **destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **dmac** *mac-addr* | **dstindex** *index-value* | **ethertype** *ethertype* | **interface** *interface* | **or-filter** [**destination-ip-address** {*ipaddr* | **ipv6** *ipaddr*}| **smac** *smac* | **source-ip-address** {*ipaddr* | **ipv6** *ipaddr*} | **srcindex** *index-value* | **vlan** *vlan-num*]

Syntax Description

and-filter	(Optional) Captures all added filters.
destination-ip-address	(Optional) Captures all packets matching a destination IP address.
ipaddr	Captures packets for a specific destination IP address.
ipv6 *ipaddr*	Captures all packets matching the IPv6 destination IP address.
dmac *mac-addr*	(Optional) Captures packets matching a destination MAC address index.
dstindex *index-value*	(Optional) Captures all packets matching a destination index; valid values are 0 to 1048575.
ethertype *ethertype*	(Optional) Captures all packets matching an ethertype; ethertype must be entered in hexidecimal format.
interface *interface*	(Optional) Captures packets related to the interface. See Usage Guidelines.
or-filter	(Optional) Applies filters.
smac *smac*	(Optional) Captures packets matching the source MAC address; smac must be entered in hexidecimal format.
source-ip-address	(Optional) Captures all packets matching a source IP address.
srcindex *index-value*	(Optional) Captures all packets matching a source index; valid values are 0 to 1048575.
vlan *vlan-num*	(Optional) Captures packets matching the VLAN number; valid VLAN numbers are 0 to 4095.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

You can use the following interface types:

- Async
- Auto-template
- CTunnel
- Dialer
- EsconPhy
- Fcpa
- Filter
- Filtergroup
- GMPLS
- GigabitEthernet
- Group-Async
- LISP
- LongReachEthernet
- Looopback
- Lspvif
- MFR
- Multilink
- Null
- Port-channel
- Sysclock
- TenGigabitEthernet
- Tunnel
- Vif
- Virtual-Ethernet
- Virtual-Template
- Virtual-TokenRing
- VLAN
- VoaBypassIn
- VoaBypassOut
- VoaFilterIn
- VoaFilterOut
- VoaIn

- VoaOut

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr capture tx

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr capture vlan

To debug NetDriver capture activity by capturing packets matching a specific VLAN number, use the **debug netdr capture vlan** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr capture vlan [*vlan-num*]

no debug netdr capture vlan [*vlan-num*]

Syntax Description

vlan-num	(Optional) Captures packets matching the VLAN number; valid VLAN numbers are 0 to 4095.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr capture

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.

Command	Description
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr clear-capture	Clears the capture buffer.
debug netdr copy-captured	Copies the packets to a file.

debug netdr clear-capture

To clear the capture buffer, use the **debug netdr clear-capture** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr clear-capture

no debug netdr clear-capture

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Examples

This example shows how to debug the NetDriver:

```
Router# debug netdr clear-capture

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.

Command	Description
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr copy-captured	Copies the packets to a file.

debug netdr copy-captured

To store captured packets to a file, use the **debug netdr copy-captured** command in Privileged EXEC mode. Use the **no** form of this command to disable debugging output.

debug netdr copy-captured

no debug netdr copy-captured

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SY	Support for this command on the Cisco 7600 series routers was extended to the 12.1 E release.

Usage Guidelines

You can copy a captured file to the following sources:

- bootdisk:
- const_nvram:
- dfc#2-bootflash:
- dfc#3-bootflash:
- disk0:
- ftp:
- http:
- https:
- image:
- null:
- nvram:
- rcp:
- scp:
- syslog:
- tftp:
- tmpsys:

Examples

This example shows how to debug the NetDriver copied packets:

```
Router# debug netdr copy-captured

Router#
```

Related Commands

Command	Description
debug netdr capture	Debugs NetDriver capture activity.
debug netdr capture and-filter	Debugs added filters.
debug netdr capture continuous	Debugs netdr continuously.
debug netdr capture destination-ip-address	Debugs all matching destination packets.
debug netdr capture dmac	Debugs matching destination packets.
debug netdr capture dstindex	Debugs packets matching destination index.
debug netdr capture ethertype	Debugs packets matching the ethertype.
debug netdr capture interface	Debugs packets related to an interface.
debug netdr capture or-filter	Debugs or-filter function packets.
debug netdr capture rx	Debugs incoming packets only.
debug netdr capture smac	Debugs packets matching the source MAC address.
debug netdr capture source-ip-address	Debugs packets matching the source IP address.
debug netdr capture srcindex	Debugs packets matching the source index.
debug netdr capture tx	Debugs outgoing packets only.
debug netdr capture vlan	Debugs packets for a specific VLAN.
debug netdr clear-capture	Clears the capture buffer.

debug platform software multicast routing

To display debug information for multicast routing software components, use the **debug platform software multicast routing** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug platform software multicast routing {**cmfib** [**all** | **error** | **event** | **stats**] | **hal** [**all** | **error** | **event**]}

no debug platform software multicast routing {**cmfib** [**all** | **error** | **event** | **stats**] | **hal** [**all** | **error** | **event**]}

Syntax Description

cmfib	Enables dubugging multicast CMFIB (Constellation multicast forwarding information base).
all	(Optional) Enables debugging for all multicast routing, events, and errors.
error	(Optional) Enables debugging multicast routing errors.
event	(Optional) Enables debugging multicast routing events.
stats	(Optional) Enables debugging multicast hardware statistics.
hal	Enables debugging multicast hardware abstraction layer (HAL).

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.1(1)SY	Support for this command was introduced.

Examples

The following example shows the multicast routing error output:

```
Router# debug platform software multicast routing cmfib error
CMFIB Error debugging is on
```

The following example shows multicast hardware statistics for HAL:

```
Router# debug platform software multicast routing hal event
Multicast HAL event log debugging is on
PE-3-sp#
*Oct 30 09:24:48.078 EDT: SP: hal_timer_event: NRPF-AG
*Oct 30 09:24:48.790 EDT: SP: hal_timer_event: S-CHECK
*Oct 30 09:24:49.754 EDT: SP: hal_timer_event: NRPF-AG
*Oct 30 09:24:51.530 EDT: SP: hal_timer_event: NRPF-AG
*Oct 30 09:24:53.298 EDT: SP: hal_timer_event: NRPF-AG
*Oct 30 09:24:55.154 EDT: SP: hal_timer_event: NRPF-AG
```

Related Commands

Command	Description
platform software met profile	Configures the number of blocks for each block size of your MET profile.
show platform hardware cef adjacencies entry	Displays a single adjacency entry index.
show platform hardware cef mpls detail	Displays MPLS CEF detail information.
show platform hardware multicast routing	Matches and displays multicast routing group IP addresses.
show platform hardware met read	Displays platform hardware MET table entries.
show platform software met detail	Displays software routing for the MET.

disconnect-timeout

To change the EXEC timeout value for the main console after the console cable is removed, use the **disconnect-timeout** command in EXEC mode.

disconnect-timeout *seconds*

Syntax Description

seconds	Number of seconds until the console connection is to be disconnected; valid values are 1 — 10 seconds.

Defaults

1 second

Command Modes

EXEC

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Usage Guidelines

You cannot save the **disconnect-timeout** command to the configuration file.

The supervisor engine automatically detects the console cable removal from the front panel console port and terminates the main console EXEC session after the specified timeout.

Examples

The following example shows how to set the disconnect time to 3 seconds:

```
Switch# disconnect-timeout 3
```

fips

To enable the Federal Information Processing Standards (FIPS) security requirements on the switch, use the **fips** command in FIPS mode.

fips

no fips

Syntax Description

This command has no keywords or arguments

Defaults

None

Syntax Description

FIPS

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Examples

This example shows how to enable FIPS security on a switch:

```
Router# fips
%FIPS mode will be enabled at next reload.
```

This example shows how to disable FIPS security on a switch:

```
Router# fips
%FIPS mode will be disabled at next reload.
```

Related Commands

Command	Description
show fips	Displays the FIPS mode.

flow hardware export

To configure Yielding NetFlow Data Export (NDE) parameters, use the **flow hardware export threshold** command in global configuration mode. To disable the export parameters, use the **no** form of this command.

flow hardware export threshold *percentage* **linecard** *percentage*

no flow hardware export threshold *percentage* **linecard** *percentage*

Syntax Description

threshold	NDE CPU threshold.
percentage	Total threshold as a percentage; valid values are 25 to 90.
linecard	NDE line card threshold.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

The following example configures the NDE CPU and line card threshold percentages to 50:

```
Router(config)# flow hardware export threshold 50
```

The following example configures the NDE CPU threshold percentage to 50 and line card threshold percentage to 70:

```
Router(config)# flow hardware export threshold 50 linecard 70
```

Related Commands

Command	Description
show platform flow export	Displays information about the hardware NDE parameters.

logging buffered

To enable system message logging to a local buffer, use the **logging buffered** command in global configuration mode. To cancel the use of the buffer, use the **no** form of this command. To return the buffer size to its default value, use the **default** form of this command.

logging buffered [**discriminator** *discr-name*] [*buffer-size*] [*severity-level*]

no logging buffered

default logging buffered

Syntax Description

discriminator	(Optional) Specifies a user-defined filter, via the logging discriminator, for syslog messages.
discr-name	(Optional) String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
buffer-size	(Optional) Size of the buffer, in bytes. The range is 4096 to 2147483647. The default size varies by platform.
severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): [**0 | emergencies**]—System is unusable [**1 | alerts**]—Immediate action needed [**2 | critical**]—Critical conditions [**3 | errors**]—Error conditions [**4 | warnings**]—Warning conditions [**5 | notifications**]—Normal but significant conditions [**6 | informational**]—Informational messages [**7 | debugging**]—Debugging messages The default logging level varies by platform but is generally 7. Level 7 means that messages at all levels (0–7) are logged to the buffer.

Command Default

Varies by platform. For most platforms, logging to the buffer is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.1(17)T	The *severity-level* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **discriminator** keyword and *discr-name* argument were added.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

This command copies logging messages to an internal buffer. The buffer is circular in nature, so newer messages overwrite older messages after the buffer is filled.

Specifying a severity-level causes messages at that level and numerically lower levels to be logged in an internal buffer.

The optional **discriminator** keyword and *discr-name* argument provide another layer of filtering that you can use to control the type and number of syslog messages that you want to receive.

When you resize the logging buffer, the existing buffer is freed and a new buffer is allocated. To prevent the router from running out of memory, do not make the buffer size too large. You can use the **show memory** EXEC command to view the free processor memory on the router; however, the memory value shown is the maximum available and should not be approached. The **default logging buffered** command resets the buffer size to the default for the platform.

On Catalyst 6500 standalone switches and Catalyst 6500 virtual switches, the default logging buffered size is 8192.

To display messages that are logged in the buffer, use the **show logging** command. The first message displayed is the oldest message in the buffer.

The **show logging** command displays the addresses and levels associated with the current logging setup and other logging statistics.

Table 1 shows a list of levels and corresponding syslog definitions.

Table 1 Error Message Logging Priorities and Corresponding Syslog Definitions

Level	Level Keyword	Syslog Definition
0	**emergencies**	LOG_EMERG
1	**alerts**	LOG_ALERT
2	**critical**	LOG_CRIT
3	**errors**	LOG_ERR
4	**warnings**	LOG_WARNING
5	**notifications**	LOG_NOTICE
6	**informational**	LOG_INFO
7	**debugging**	LOG_DEBUG

Examples

The following example shows how to enable standard system logging to the local syslog buffer:

```
Router(config)# logging buffered
```

The following example shows how to use a message discriminator named buffer1 to filter critical messages, meaning that messages at levels 0, 1, and 2 are filtered:

```
Router(config)# logging buffered discriminator buffer1 critical
```

Related Commands

Command	Description
clear logging	Clears messages from the logging buffer.
logging buffered xml	Enables system message logging (syslog) and sends XML-formatted logging messages to the XML-specific system buffer.
show logging	Displays the syslog.

mac address-table aging-time

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

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

no mac address-table aging-time *seconds* [**routed-mac** | **vlan** *vlan-id*]

Syntax Description

seconds	MAC address table entry maximum age. Valid values are 0 and from 5 to 1000000 seconds. Aging time is counted from the last time that the switch detected the MAC address. The default value is 300 seconds.
vlan *vlan-id*	(Optional) Specifies the VLAN to apply the changed aging time; valid values are from 1 to 4094.

Command Default

The default aging time is 300 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

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

Enter 0 seconds to disable aging.

Examples

The following example shows how to configure the aging time:

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

The following example shows how to disable the aging time:

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

Related Commands

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

mac address-table aging-type

To add routed addresses to the MAC address table, use the **mac address-table aging-type** command in global configuration mode. To remove routed entries from the MAC address table, use the **no** form of this command.

mac address-table routed-mac

no mac address-table routed-mac

Syntax Description

routed-mac	Specifies routed MAC address entries.

Command Default

Dynamic addresses are not added to the MAC address table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

The following example shows how to add a MAC address on port fa1/1 to VLAN 4:

```
Switch(config)# mac address-table aging-type 4
```

Related Commands

Command	Description
clear mac address-table	Deletes entries from the MAC address table.
mac address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
mac address-table static	Adds static addresses to the MAC address table.
show mac address-table	Displays the MAC address table.

mac address-table learning

To enable MAC address learning, use the **mac address-table learning** command in global configuration mode. To disable learning, use the **no** form of this command.

[**default**] **mac address-table learning** {**vlan** *vlan-id* | **interface** *interface slot/port*} [**module** *num*]

no mac address-table learning {**vlan** *vlan-id* | **interface** *interface slot/port*} [**module** *num*]

Syntax Description

default	(Optional) Returns to the default settings.
vlan *vlan-id*	Specifies the VLAN to apply the per-VLAN learning of all MAC addresses; valid values are from 1 to 4094.
interface	Specifies per-interface based learning of all MAC addresses.
interface slot/port	Interface type, the slot number, and the port number.
module *num*	(Optional) Specifies the module number.

Defaults

If you configure a VLAN on a port in a module, all of the supervisor engines and Distributed Forwarding Cards (DFCs) in the Cisco 7600 series router are enabled to learn all the MAC addresses on the specified VLAN.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

You can use the **module** *num* keyword and argument to specify supervisor engines or DFCs only.

You can use the **vlan** *vlan-id* keyword and argument on switch port VLANs only. You cannot use the **vlan** *vlan-id* keyword and argument to configure learning on routed interfaces.

You can use the **interface** *interface slot/port* keyword and arguments on routed interfaces, supervisor engines, and DFCs only. You cannot use the **interface** *interface slot/port* keyword and arguments to configure learning on switch port interfaces or non-DFC modules.

Examples

This example shows how to enable MAC address learning on a switch port interface on all modules:

```
Router(config)# mac address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC address learning on a switch port interface on a specified module:

```
Router(config)# mac address-table learning vlan 100 module 4
Router(config)#
```

This example shows how to disable MAC address learning on a specified switch-port interface for all modules:

```
Router(config)# no mac address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC address learning on a routed interface on all modules:

```
Router(config)# mac address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC address learning on a routed interface for a specific module:

```
Router(config)# mac address-table learning interface FastEthernet 3/48 module 4
Router(config)#
```

This example shows how to disable MAC address learning for all modules on a specific routed interface:

```
Router(config)# no mac address-table learning interface FastEthernet 3/48
Router(config)#
```

Related Commands

Command	Description
show mac address-table learning	Displays the MAC address learning state.

mac address-table limit

To enable the MAC limiting functionality and set the limit to be imposed, use the **mac address-table limit** command in global configuration mode. To disable MAC limiting, use the **no** form of this command.

mac address-table limit [**action** {**warning** | **limit** | **shutdown**}] [**notification** {**syslog** | **trap** | **both**}] [**interface** *type mod/port*] [**maximum** *num*] [**vlan** *vlan*] [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

no mac address-table limit [**action** {**warning** | **limit** | **shutdown**}] [**notification** {**syslog** | **trap** | **both**}] [**interface** *type mod/port*] [**maximum** *num*] [**vlan** *vlan*] [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

Syntax Description

action	(Optional) Specifies the type of action to be taken when the action is violated.
warning	(Optional) Specifies that the one syslog message will be sent and no further action will be taken when the action is violated.
limit	(Optional) Specifies that the one syslog message will be sent and/or a corresponding trap will be generated with the MAC limit when the action is violated.
shutdown	(Optional) Specifies that the one syslog message will be sent and/or the VLAN is moved to the blocked state when the action is violated.
notification	(Optional) Specifies the type of notification to be sent when the action is violated.
syslog	(Optional) Sends a syslog message when the action is violated.
trap	(Optional) Sends trap notifications when the action is violated.
both	(Optional) Sends syslog and trap notifications when the action is violated.
interface *type mod/port*	(Optional) Enables MAC limiting on a per-port basis.
maximum *num*	(Optional) Specifies the maximum number of MAC entries per-VLAN per-Encoded Address Recognition Logic (EARL) allowed; valid values are from 5 to 32768 mac address entries.
vlan *vlan*	(Optional) Enables MAC limiting on a per-VLAN basis.
flood	(Optional) Enables unknown unicast flooding on a VLAN.

Defaults

The defaults are as follows:

- **maximum** *num* is 500 MAC address entries.
- **action** is **warning**.
- **notification** is **syslog**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

MAC limiting can be enabled on either a per-interface basis (by specifying an interface) or on a per-VLAN basis (by specifying a VLAN). However, MAC limiting must first be enabled for the router (a higher level) in global configuration mode (config).

General Guidelines About MAC Limiting

Note the following guidelines about enabling MAC limiting:

- The maximum number of MAC entries is determined on a per-VLAN and per-EARL basis.
- If you do not specify a maximum number, an action, or a notification, the default settings are used.
- If you enable per-VLAN MAC limiting, MAC limiting is enabled on the specified VLAN only.
- The **flood** keyword is supported on VLAN interfaces only.
- The **flood** action occurs only if the **limit** action is configured and is violated.
- In the **shutdown** state, the VLAN remains in the blocked state until you reenable it through the command syntax.

Syntax for Enabling per-VLAN MAC Limiting

The following is sample syntax that can be used to enable per-VLAN MAC limiting. Both the **mac address-table limit** and **mac address-table limit vlan** commands must be used to properly enable per-VLAN MAC limiting.

mac address-table limit

Note This command enables the MAC limiting functionality for the router.

mac address-table limit [**maximum** *num*] [**vlan** *vlan*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

Note This command sets the specific limit and any optional actions to be imposed at the VLAN level.

Syntax for Enabling Per-Interface MAC Limiting

The following is sample syntax that can be used to enable per-interface MAC limiting. Both the **mac address-table limit** and **mac address-table limit interface** commands commands must be used to properly enable per-interface MAC limiting.

mac address-table limit

Note This command enables the MAC limiting functionality for the router.

mac address-table limit [**interface** *type mod/port*] [**maximum** *num*] [**action** {**warning** | **limit** | **shutdown**}] [**flood**]

Note This command sets the specific limit and any optional actions to be imposed at the interface level.

Examples

This example shows how to enable per-VLAN MAC limiting. The first instance of the **mac address-table limit** command enables MAC limiting. The second instance of the command sets the limit and any optional actions to be imposed at the VLAN level.

```
Router# enable
Router# configure terminal
Router(config)# mac address-table limit
Router(config)# mac address-table limit vlan 501 maximum 50 action shutdown
Router(config)# end
```

This example shows how to enable per-interface MAC limiting. The first instance of the **mac address-table limit** command enables MAC limiting. The second instance of the command sets the limit and any optional actions to be imposed at the interface level.

```
Router# enable
Router# configure terminal
Router(config)# mac address-table limit
Router(config)# mac address-table limit fastethernet0/0 maximum 50 action shutdown
Router(config)# end
```

Related Commands

Command	Description
show mac address-table limit	Displays the information about the MAC address table.

mac address-table notification change

To send a notification of the dynamic changes to the MAC address table, use the **mac address-table notification change** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mac address-table notification change [**history** *size* | **interval** *seconds*]

no mac address-table notification change [**history** *size* | **interval** *seconds*]

Syntax Description

history *size*	(Optional) Sets the number of entries in the history buffer; valid values are from 0 to 500 entries.
interval *seconds*	(Optional) Sets the minimum change sending interval; valid values are from 0 to 2147483647 seconds.

Command Default

The default settings are as follows:

- Disabled
- If notification of the dynamic changes to the MAC address table is enabled, the default settings are as follows:
  - **histor**y *size* is 1 entry.
  - **interval** *value* is 1 second.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

This example shows how to configure the Simple Network Management Protocol (SNMP) notification of dynamic additions to the MAC address table of addresses:

```
Router(config)# mac address-table notification change interval 5 history 25
```

Related Commands

Command	Description
show mac address-table	Displays information about the MAC address table.
snmp-server trap mac-notification	Enables the SNMP trap notification on a LAN port when MAC addresses are added to or removed from the address table.

mac address-table notification mac-move

To enable MAC-move notification, use the **mac address-table notification mac-move** command in global configuration mode. To disable MAC-move notification, use the **no** form of this command.

mac address-table notification mac-move [**counter** [**syslog**]]

no mac address-table notification mac-move [**counter** [**syslog**]]

Syntax Description

counter	(Optional) Specifies the MAC-move counter feature.
syslog	(Optional) Specifies the syslog facility when the MAC-move notification detects the first instance of the MAC move.

Command Default

MAC-move notification is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

MAC-move notification generates a syslog message whenever a MAC address or host moves between different switch ports.

MAC-move notification does not generate a notification when a new MAC address is added to the content-addressable memory (CAM) or when a MAC address is removed from the CAM.

MAC-move notification is supported on switch ports only.

The MAC-move counter notification generates a syslog message when the number of MAC moves in a VLAN exceeds the maximum limit. The maximum limit is 1000 MAC moves.

The MAC-move counter syslog notification counts the number of times a MAC has moved within a VLAN and the number of these instances that have occurred in the system.

Examples

This example shows how to enable MAC-move notification:

```
Router(config)# mac address-table notification mac-move
```

This example shows how to disable MAC-move notification:

```
Router(config)# no mac address-table notification mac-move
```

This example shows how to enable MAC-move counter syslog notification:

```
Router(config)# mac address-table notification mac-move counter syslog
```

This example shows how to disable MAC-move counter notification:

```
Router(config)# no mac address-table notification mac-move counter
```

Related Commands

Command	Description
clear mac address-table notification mac-move	Clears the MAC address table notification counters.
show mac address-table notification mac-move	Displays the information about the MAC address table.

mac address-table static

To add static entries to the MAC address table or to disable Internet Group Multicast Protocol (IGMP) snooping for a particular static multicast MAC address, use the **mac address-table static** command in global configuration mode. To remove entries profiled by the combination of specified entry information, use the **no** form of this command.

mac address-table static *mac address* **vlan** *vlan-id* {**interface** *int* | **drop** [**disable-snooping**]} [**dlci** *dlci* | **pvc** *vpi*/*vci*] [**auto-learn** | **disable-snooping**] [**protocol** {**ip** | **ipx** | **assigned**}]

no mac address-table static *mac address* **vlan** *vlan-id* {**interface** *int* | **drop** [**disable-snooping**]} [**dlci** *dlci* | **pvc** *vpi*/*vci*] [**auto-learn** | **disable-snooping**] [**protocol** {**ip** | **ipx** | **assigned**}]

Syntax Description

mac address	Address to add to the MAC address table.
vlan *vlan-id*	Specifies the VLAN associated with the MAC address entry. The range is from 2 to 100.
interface *int*	Specifies the interface type and the slot and port to be configured. The *int* argument should specify the interface *type* and the *slot*/*port* or *slot*/*subslot*/*port* numbers (for example, **interface pos 5/0** or **interface atm 8/0/1**).
drop	Drops all traffic that is received from and going to the configured MAC address in the specified VLAN.
disable-snooping	(Optional) Disables IGMP snooping on the multicast MAC address.
dlci *dlci*	(Optional) Specifies the data-link connection identifier (DLCI) to be mapped to this MAC address. The valid range is from 16 to 1007. **Note** This option is valid only if Frame Relay encapsulation has been enabled on the specified interface.
pvc *vpi*/*vci*	(Optional) Specifies the permanent virtual circuit (PVC) to be mapped to this MAC address. You must specify both a virtual path identifier (VPI) and a virtual circuit identifier (VCI), separated by a slash. **Note** This option is valid only for ATM interfaces.
auto-learn	(Optional) Specifies that if the router sees this same MAC address on a different port, the MAC entry should be updated with the new port.
disable-snooping	(Optional) Disables IGMP snooping on the Frame Relay DLCI or ATM PVC.
protocol	(Optional) Specifies the protocol associated with the entry.
ip	(Optional) Specifies the IP protocol.
ipx	(Optional) Specifies the Internetwork Packet Exchange (IPX) protocol.
assigned	(Optional) Specifies assigned protocol bucket accounts for protocols such as DECnet, Banyan VINES, and AppleTalk.

Command Default

Static entries are not added to the MAC address table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

The output interface specified cannot be an SVI.

We recommend configuring static MAC addresses on Layer 2 EtherChannels only and not on Layer 2 physical member ports of an EtherChannel. This action does not apply to Layer 3 EtherChannels and its members.

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

- Remove entries that are profiled by the combination of specified entry information.
- Reenable IGMP snooping for the specified address.

The **dlci** *dlci* keyword and argument are valid only if Frame Relay encapsulation has been enabled on the specified interface.

The **pvc** *vpi*/*vci* keyword and arguments are supported on ATM interfaces only. When specifying the **pvc** *vpi*/*vci*, you must specify both a VPI and a VCI, separated by a slash.

When you install a static MAC address, it is associated with a port. If the same MAC address is seen on a different port, the entry is updated with the new port if you enter the **auto-learn** keyword.

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

The **ipx** keyword is not supported.

You can enter up to 15 interfaces per command entered, but you can enter more interfaces by repeating the command.

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

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

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

The **mac address-table static** *mac address* **vlan** *vlan-id* **interface** *int* **disable-snooping** command disables snooping on the specified static MAC address/VLAN pair only. To reenable snooping, first you must delete the MAC address using the **no** form of the command, and then you must reinstall the MAC address using the **mac address-table static** *mac address* **vlan** *vlan-id* **interface** *int* command, without entering the **disable-snooping** keyword.

The **mac address-table static** *mac address* **vlan** *vlan-id* **drop** command cannot be applied to a multicast MAC address.

Note Both the unicast MAC addresses and the multicast MAC addresses allow only one WAN interface.

Specifying a MAC Address for DLCI or PVC Circuits

To support multipoint bridging and other features, the behavior of the following command has changed for ATM and Frame Relay interfaces in Cisco IOS Release 12.2(18)SXE and later releases. In previous releases, you needed to specify only a VLAN ID and an interface.

```
Router(config)# mac address-table static 000C.0203.0405 vlan 101 interface ATM6/1
```

In Cisco IOS Release 12.2(18)SXE, you must also specify the **dlci** option for Frame Relay interfaces, or the **pvc** option for ATM interfaces, such as in the following example:

```
Router(config)# mac address-table static 000C.0203.0405 vlan 101 interface ATM6/1 pvc6/101
```

Note If you omit the **dlci** option for Frame Relay interfaces, the MAC address is mapped to the first DLCI circuit that is configured for the specified VLAN on that interface. Similarly, if you omit the **pvc** option for ATM interfaces, the MAC address is mapped to the first PVC that is configured for the specified VLAN on that interface. To ensure that the MAC address is configured correctly, we recommend always using the **dlci** and **pvc** keywords on the appropriate interfaces.

Examples

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

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

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

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

The following example shows how to add static entries to the MAC address table for an ATM PVC circuit and for a Frame Relay DLCI circuit:

```
Router(config)# mac address-table static 0C01.0203.0405 vlan 101 interface ATM6/1 pvc
6/101
Router(config)# mac address-table static 0C01.0203.0406 vlan 202 interface POS4/2 dlci 200
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for a specific MAC address.

mac address-table synchronize

To synchronize the Layer 2 MAC address table entries across the Policy Feature Card (PFC) and all the Distributed Forwarding Cards (DFCs), use the **mac address-table synchronize** command in global configuration mode. To disable MAC address table synchronization or reset the activity timer, use the **no** form of this command.

mac address-table synchronize [**activity-time** *seconds* | **auto**]

no mac address-table synchronize [**activity-time** *seconds* | **auto**]

Syntax Description

activity-time *seconds*	(Optional) Specifies the activity timer interval: valid values are 160, 320, and 640 seconds.
auto	(Optional) Specifies that MAC address synchronization occur automatically.

Defaults

The default settings are as follows:

- Layer 2 MAC address table entries are not synchronized by default.
- Enabled for WS-X6708-10GE.
- If the command is enabled, the value of the **activity-time** keyword is 160 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

We recommend that you configure the activity time so that at least two activity times exist within the regular Layer 2 aging time (or within the aging time used for VLANs in distributed EtherChannels if this feature is used only for distributed EtherChannels). If at least two activity times do not exist within the aging time, then an error message is displayed.

Examples

This example shows how to specify the activity timer interval:

```
Router(config)# mac address-table synchronization activity time 160
Router(config)#
```

This example shows how to specify the activity timer interval when out-of-band (OOB) synchronization is enabled:

```
Router(config)# mac address-table synchronization activity time 160
 % Current OOB activity time is [160] seconds
 % Recommended aging time for all vlans is atleast three times the activity interval and
 global aging time will be changed automatically if required
Router(config)#
```

This example shows how to display the timer interval:

```
Router(config)# mac address-table synchronization
Router(config)#
```

This example shows how to display the timer interval when OOB synchronization is enabled:

```
Router(config)# mac address-table synchronization
 % Current OOB activity time is [160] seconds
 % Recommended aging time for all vlans is atleast three times the activity interval
Router(config)#
```

Related Commandsa

Command	Description
show mac address-table synchronize statistics	Displays information about the MAC address table.

match l2 miss

To match Layer 2 MAC miss in ingress policy, use the **match l2 miss** command.

match l2 miss

Command Default

This command has no default settings.

Command Modes

Class Map configuration

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

The following example shows how to obtain information on match layer 2 MAC miss in ingress policy:

```
Router(config-cmap)# match l2 miss
```

mls ip multicast half-met

To halve the multicast expansion table (MET), use the **mls ip multicast half-met** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls ip multicast half-met

no mls ip multicast half-met

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

Global configuration mode

Command History

Release	Modification
15.1(1)SY	Support for this command was introduced.

Usage Guidelines

The **mls ip multicast half-met** command replaces the **ipv6 mfib hardware-switching uplink** command.

The **mls ip multicast half-met** command is required for supporting IPv6 multicast on the redundant Supervisor Engine 720 and Supervisor Engine 720-10GE. The command is applicable only on reload.

Examples

This example shows how to enable halve the MET:

```
Router(config)# mls ip multicast half-met
```

This example shows how to disablethe halve the MET:

```
Router# no mls ip multicast half-met
```

Related Commands

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

monitor session type

To configure a local Switched Port Analyzer (SPAN), RSPAN, or ERSPAN, use the **monitor session type** command in global configuration mode. To remove one or more source or destination interfaces from the SPAN session, use the **no** form of this command.

monitor session *span-session-number* **type** {**erspan-destination | erspan-source | local | local-tx | rspan-destination | rspan-source**}

no monitor session *span-session-number* **type** {**erspan-destination | erspan-source | local | local-tx | rspan-destination | rspan-source**}

Syntax Description

span-session-number	Number of the local SPAN or ERSPAN session; valid values are from 1 to 66.
erspan-destination	Specifies the ERSPAN destination-session configuration mode.
erspan-source	Specifies the ERSPAN source-session configuration mode.
local	Specifies the local SPAN session configuration mode.
local-tx	Specifies the local egress-only SPAN session configuration mode.
rspan-destination	Specifies the RSPAN destination-session configuration mode.
rspan-source	Specifies the RSPAN source-session configuration mode.

Defaults

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced.
12.2(18)SXF	This command was changed to support ERSPAN in any switch fabric module functionality switching mode.
12.2(33)SXH	This command was changed to include the following keywords: • **local** • **local-tx** • **rspan-destination** • **rspan-source**
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY. Cisco IOS Release 12.2(50)SY does not support the **source cpu** keyword.

Usage Guidelines

Release 12.2(18)SXE and later releases support ERSPAN with the Supervisor Engine 720, hardware revision 3.2 or higher. Enter the **show module version | include WS-SUP720-BASE** command to display the hardware revision.

ERSPAN traffic is GRE-encapsulated SPAN traffic that can only be processed by an ERSPAN destination session.

This command is not supported on Catalyst 6500 series switches that are configured with a Supervisor Engine 2.

All ERSPAN source sessions on a switch must use the same source IP address. You enter the **origin ip address** command to configure the IP address for the ERSPAN source sessions.

All ERSPAN destination sessions on a switch must use the same IP address. You enter the **ip address** command to configure the IP address for the ERSPAN destination sessions. If the ERSPAN destination IP address is not a PFC3 mode switch (for example, it is a network sniffer), the traffic arrives with the GRE and RSPAN headers/encapsulation intact.

The ERSPAN source session destination IP address, which must be configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to the destination ports. You configure the same address in both the source and destination sessions with the **ip address** command.

The ERSPAN ID differentiates the ERSPAN traffic arriving at the same destination IP address from different ERSPAN source sessions.

The local ERSPAN session limits are as follows:

- Total sessions—66
- Source sessions—2 (ingress or egress or both)
- Destination sessions—23

The **monitor session type** command creates a new ERSPAN session or allows you to enter the ERSPAN session configuration mode. ERSPAN uses separate source and destination sessions. You configure the source and destination sessions on different switches. The ERSPAN session configuration mode prompts are as follows:

- Router(config-mon-erspan-src)—Indicates the ERSPAN source session configuration mode.
- Router(config-mon-erspan-src-dst)—Indicates the ERSPAN source session destination configuration mode.
- Router(config-mon-erspan-dst)—Indicates the ERSPAN destination session configuration mode.
- Router(config-mon-erspan-dst-src)—Indicates the ERSPAN destination session source configuration mode

Table 2 lists the ERSPAN destination session configuration mode syntaxes.

Table 2 ERSPAN Destination Session Configuration Mode Syntaxes

Syntax	Description
Global Configuration Mode	

monitor session *erspan-destination-session-number* | *rspan-destination-session-number* **type erspan-destination** | **erspan-destination**	Enters ERSPAN or RSPAN destination session configuration mode and changes the prompt to the following:
	`Router(config-mon-erspan-dst)#`
	`Router(config-mon-rspan-dst)#`

Destination Session Configuration Mode	
description *session-description*	(Optional) Describes the ERSPAN or RSPAN destination session.

Table 2 ERSPAN Destination Session Configuration Mode Syntaxes

Syntax	Description
shutdown	(Optional) (Default) Inactivates the ERSPAN destination session.
no shutdown	Activates the ERSPAN destination session.
destination {*single-interface* | *interface-list* | *interface-range* | *mixed-interface-list*}	Associates the ERSPAN destination session number with the destination ports.
source	Enters ERSPAN destination session source configuration mode and changes the prompt to the following: `Router(config-mon-erspan-dst-src)#`
Destination Session Source Configuration Mode	
ip address *ip-address* [**force**]	Configures the ERSPAN flow destination IP address, which must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.
erspan-id *erspan-flow-id*	Configures the ID number used by the destination and destination sessions to identify the ERSPAN traffic.
vrf *vrf-name*	(Optional) Configures the VRF name of the packets in the ERSPAN traffic.

Table 3 lists the ERSPAN source session configuration mode syntaxes.

Table 3 ERSPAN or RSPAN Source Session Configuration Mode Syntaxes

Syntax	Description
Global Configuration Mode	

monitor session *erspan-source-session-number* **type erspan-source | rspan-source**	Enters ERSPAN or RSPAN source session configuration mode and changes the prompt as appropriate to the following:
	`Router(config-mon-erspan-src)#`
	`Router(config-mon-rspan-src)#`

Source Session Configuration Mode	
description *session-description*	(Optional) Describes the ERSPAN or RSPAN source session.
shutdown	(Optional) (Default) Inactivates the ERSPAN or RSPAN source session.
no shutdown	Activates the ERSPAN or RSPAN source session.
source {{*single-interface* | *interface-list* | *interface-range* | *mixed-interface-list* | *single-vlan* | *vlan-list* | *vlan-range* | *mixed-vlan-list*} [**rx** | **tx** | **both**]}	Associates the ERSPAN or RSPAN source session number with the source ports or VLANs, and selects the traffic direction to be monitored.
filter {*single-vlan* | *vlan-list* | *vlan-range* | *mixed-vlan-list*}	(Optional) Configures source VLAN filtering when the ERSPAN or RSPAN source is a trunk port.
description *session-description*	(Optional) Describes the ERSPAN or RSPAN source session.

Table 3 ERSPAN or RSPAN Source Session Configuration Mode Syntaxes

Syntax	Description
Source Session Destination Configuration Mode	
ip address *ip-address*	Configures the ERSPAN or RSPAN flow destination IP address, which must also be configured on an interface on the destination switch and be entered in the ERSPAN or RSPAN destination session configuration.
erspan-id *erspan-flow-id*	Configures the ID number used by the source and destination sessions to identify the ERSPAN or RSPAN traffic.
origin ip address *ip-address*	Configures the IP address used as the source of the ERSPAN or RSPAN traffic.
ip {{**ttl** *ttl-value*} | {**prec** *ipp-value*} | {**dscp** *dscp-value*}}	(Optional) Configures the following packet values in the ERSPAN or RSPAN traffic: • **ttl** *ttl-value*—IP time-to-live (TTL) value • **prec** *ipp-value*—IP-precedence value • **dscp** *dscp-value*—IP-precedence value
vrf *vrf-name*	(Optional) Configures the VRF name of the packets in the ERSPAN or RSPAN traffic.

When you configure the monitor sessions, follow these syntax guidelines:

- *erspan-destination-span-session-number* can range from 1 to 66.
- *single-interface* is **interface** *type slot/port*; *type* is **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface-list* is *single-interface* , *single-interface* , *single-interface* ...

Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface-range* is **interface** *type slot/first-port - last-port* .
- *mixed-interface-list* is, in any order, *single-interface* , *interface-range* , ...
- *erspan-flow-id* can range from 1 to 1023.

When you clear the monitor sessions, follow these syntax guidelines:

- The **no monitor session** *session-number* command entered with no other parameters clears the session *session-number.*
- *session-range* is *first-session-number-last-session-number.*

Note When you enter the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

Use the **monitor session type local** command to configure ingress, egress, or both ingress and egress SPAN sessions.

Use the **monitor session type local-tx** command to configure egress-only SPAN sessions.

When you enter the local or the local egress-only SPAN session configuration mode, the prompt changes accordingly to Router(config-mon-local)# or Router(config-mon-local-tx)#, and the following commands are available:

- **description**—Describes the properties for this session using this syntax:

  description *description*

  The *description* can be up to 240 characters and cannot contain special characters or spaces.

- **destination**—Specifies the destination and the destination properties using this syntax:

  destination {**analysis-module** *num* | **anomaly-detector-module** *num* | **interface** *type number* | **intrusion-detection-module** *num*}

analysis-module *num*	Specifies the SPAN destination analysis-module.
anomaly-detector-module *num*	Specifies the SPAN destination anomaly-detector-module.
interface *type number*	Specifies the **interface** *type* and *number* as follows: • **GigabitEthernet** *mod/port* • **port-channel** *num*—Ethernet Channel of interfaces; valid values are from 1 to 496.
ingress	(Optional) Configures destinations to receive traffic from attached devices.
learning	(Optional) Enables MAC address learning from the destinations, which allows the switch to transmit traffic that is addressed to devices attached to the destinations.
intrusion-detection-module *num*	Specifies the SPAN destination intrusion-detection-module.

- **exit**—Exits from configuration session mode.
- **filter vlan** *vlan-id*—Limits the SPAN source traffic to specific VLANs; valid values are from 1 to 4096.
- **no**—Negates a command or sets its defaults.
- **shutdown**—Shuts down this session
- **source**—Specifies the SPAN source interface or VLAN using the following syntax:

  source {**cpu** {**rp** | **sp**} | {**interface** *type number*} | {**intrusion-detection-module** *num*} | {**vlan** *vlan-id*}} [**,** | **-** | **rx** | **tx** | **both**]

cpu rp	Associates the local SPAN session number with the CPU on the route processor.
cpu sp	Associates the local SPAN session number with the CPU on the switch processor.

interface *type number*	Specifies the interface type and number as follows: • **FastEthernet** *mod/port* • **GigabitEthernet** *mod/port* • **Port-channel** *num*—Ethernet Channel of interfaces; valid values are from 1 to 496.
vlan *vlan-id*	Specifies the VLAN; valid values are from 1 to 4094.
,	(Optional) Specifies another range of interfaces.
-	(Optional) Specifies a range of interfaces.
both	(Optional) Monitors the received and the transmitted traffic.
rx	(Optional) Monitors the received traffic only.
tx[1]	(Optional) Monitors the transmitted traffic only.

1. When you enter the **local-tx** keyword, the **rx** and **both** keywords are not available and the **tx** keyword is required.

The local SPAN session limits are as follows:

- Total sessions—80
- Source sessions—2 (ingress or egress or both)
- Egress only—14

If you enter the **filter** keyword on a monitored trunk interface, only traffic on the set of specified VLANs is monitored.

Only one destination per SPAN session is supported. If you attempt to add another destination interface to a session that already has a destination interface configured, you get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

You can configure up to 64 SPAN destination interfaces, but you can have one egress SPAN source interface and up to 128 ingress source interfaces only.

A SPAN session can either monitor VLANs or monitor individual interfaces, but it cannot monitor both specific interfaces and specific VLANs. Configuring a SPAN session with a source interface and then trying to add a source VLAN to the same SPAN session causes an error. Configuring a SPAN session with a source VLAN and then trying to add a source interface to that session also causes an error. You must first clear any sources for a SPAN session before switching to another type of source.

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.

When you configure the **destination**, use these guidelines:

- A *single-interface* is as follows:
  - **interface** *type slot/port*; *type* is **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
  - **interface port-channel** *number*

Note Destination port channel interfaces must be configured with the **channel-group** *group-num* **mode on** command and the **no channel-protocol** command.

- An *interface-list* is *single-interface* , single-*interface* , *single-interface* ...

Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- An *interface-range* is **interface** *type slot/first-port* **-** *last-port*.
- A *mixed-interface-list* is, in any order, *single-interface* **,** *interface-range* **,** ...
- A *single-vlan* is the ID number of a single VLAN.
- A *single-list* is *single-vlan* **,** *single-vlan* **,** *single-vlan* ...
- A *vlan-range* is *first-vlan-ID* **-** *last-vlan-ID*.
- A *mixed-vlan-list* is, in any order, *single-vlan* , *vlan-range* , ...

When you clear the monitor sessions, follow these syntax guidelines:

- The **no monitor session** *session-number* command entered with no other parameters clears the session *session-number.*
- *session-range* is *first-session-number-last-session-number.*

Note When you enter the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

Examples

This example shows how to configure an ERSPAN source session number and enter the ERSPAN source session configuration mode for the session:

```
Router(config)# monitor session 55 type erspan-source
Router(config-mon-erspan-src)#
```

This example shows how to configure an ERSPAN destination session number and enter the ERSPAN destination session configuration mode for the session:

```
Router(config)# monitor session 55 type erspan-destination
Router(config-mon-erspan-dst)#
```

This example shows how to associate the ERSPAN destination session number with the destination ports:

```
Router(config-mon-erspan-dst) destination interface fastethernet 1/2 , 2/3
```

This example shows how to enter the ERSPAN destination session source configuration:

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

This example shows how to enter the ERSPAN destination session source configuration mode:

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

This example shows how to configure multiple sources for a session:

```
Router(config-mon-erspan-src)# source interface fastethernet 5/15 , 7/3 rx
Router(config-mon-erspan-src)# source interface gigabitethernet 1/2 tx
Router(config-mon-erspan-src)# source interface port-channel 102
Router(config-mon-erspan-src)# source filter vlan 2 - 3
Router(config-mon-erspan-src)#
```

This example shows how to enter the ERSPAN source session destination configuration mode:

```
Router(config-mon-erspan-src)# destination
Router(config-mon-erspan-src-dst)#
```

This example shows how to configure the ID number that is used by the source and destination sessions to identify the ERSPAN traffic:

```
Router(config-mon-erspan-src-dst)# erspan-id 1005
Router(config-mon-erspan-src-dst)#
```

This example shows how to configure session 1 to monitor ingress traffic from Gigabit Ethernet port 1/1 and configure Gigabit Ethernet port 1/2 as the destination:

```
Router(config)# monitor session 1 type local
Router(config-mon-local)# source interface gigabitethernet 1/1 rx
Router(config-mon-local)# destination interface gigabitethernet 1/2
```

This example shows how to configure session 1 to monitor egress-only traffic from Gigabit Ethernet port 5/1 and configure Gigabit Ethernet port 5/2 as the destination:

```
Router(config)# monitor session 1 type local-tx
Router(config-mon-local)# source interface gigabitethernet 5/1 rx
Router(config-mon-local)# destination interface gigabitethernet 5/2
```

This example shows how to remove an interface from a session:

```
Router(config)# no monitor session 1 type local-tx
```

Related Commands

Command	Description
monitor session type	Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.
show monitor session	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

mvr (global configuration)

To enable the multicast VLAN registration (MVR) feature on the switch, use the **mvr** global configuration command without keywords on the switch stack or on a standalone switch. Use the **no** form of this command to return to the default settings.

mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

no mvr [**group** *ip-address* | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

Syntax Description

group *ip-address*	(Optional) Statically configures an MVR group IP multicast address on the switch. Use the **no** form of this command to remove a statically configured IP multicast address or contiguous addresses or, when no IP address is entered, to remove all statically configured MVR IP multicast addresses.
count	(Optional) Configures multiple contiguous MVR group addresses. The range is 1 to 256; the default is 1.
mode	(Optional) Specifies the MVR mode of operation. The default is compatible mode.
compatible	(Optional) Sets MVR mode to provide compatibility with Catalyst 2900 XL and Catalyst 3500 XL switches. This mode does not allow dynamic membership joins on source ports.
dynamic	(Optional) Sets MVR mode to allow dynamic MVR membership on source ports.
querytime *value*	(Optional) Sets the maximum time to wait for IGMP report memberships on a receiver port. This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR querytime for an IGMP group membership report before removing the port from multicast group membership. The value is the response time in units of tenths of a second. The range is 1 to 100; the default is 5 tenths or one-half second. Use the **no** form of the command to return to the default setting.
vlan *vlan-id*	(Optional) Specifies the VLAN on which MVR multicast data is expected to be received. This is also the VLAN to which all the source ports belong. The range is 1 to 4094; the default is VLAN 1.

Defaults

MVR is disabled by default.

The default MVR mode is compatible mode.

No IP multicast addresses are configured on the switch by default.

The default group IP address count is 0.

The default query response time is 5 tenths of or one-half second.

The default multicast VLAN for MVR is VLAN 1.

Command Modes Global configuration

Command History

Release	Modification
15.0(1)SY	This command was introduced.

Usage Guidelines Use the **mvr** command with keywords to set the MVR mode for a switch, configure the MVR IP multicast address, set the maximum time to wait for a query reply before removing a port from group membership, and to specify the MVR multicast VLAN. A maximum of 256 MVR multicast groups can be configured on a switch.

Use the **mvr group** command to statically set up all the IP multicast addresses that will take part in MVR. Any multicast data sent to a configured multicast address is sent to all the source ports on the switch and to all receiver ports that have registered to receive data on that IP multicast address.

MVR supports aliased IP multicast addresses on the switch. However, if the switch is interoperating with Catalyst 6500 Series switches, you should not configure IP addresses that create an alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).

The **mvr querytime** command applies only to receiver ports.

If the switch MVR is interoperating with Catalyst 6500 Series switches, set the multicast mode to compatible.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

MVR can coexist with IGMP snooping on a switch.

Multicast routing and MVR cannot coexist on a switch. If you enable multicast routing and a multicast routing protocol while MVR is enabled, MVR is disabled and a warning message appears. If you try to enable MVR while multicast routing and a multicast routing protocol are enabled, the operation to enable MVR is cancelled and an Error message is displayed.

Examples This example shows how to enable MVR:

```
Switch(config)# mvr
```

Use the **show mvr** privileged EXEC command to display the current setting for maximum multicast groups.

This example shows how to configure 228.1.23.4 as an IP multicast address:

```
Switch(config)# mvr group 228.1.23.4
```

This example shows how to configure ten contiguous IP multicast groups with multicast addresses from 228.1.23.1 to 228.1.23.10:

```
Switch(config)# mvr group 228.1.23.1 10
```

Use the **show mvr members** privileged EXEC command to display the IP multicast group addresses configured on the switch.

This example shows how to set the maximum query response time as one second (10 tenths):

```
Switch(config)# mvr querytime 10
```

This example shows how to set VLAN 2 as the multicast VLAN:

```
Switch(config)# mvr vlan 2
```

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

Related Commands

Command	Description
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays MVR global parameters or port parameters.
show mvr interface	Displays the configured MVR interfaces with their type, status, and Immediate Leave configuration. Also displays all MVR groups of which the interface is a member.
show mvr members	Displays all ports that are members of an MVR multicast group; if the group has no members, its status is shown as Inactive.

mvr (interface configuration)

To configure a Layer 2 port as a multicast VLAN registration (MVR) receiver or source port, to set the Immediate Leave feature, and to statically assign a port to an IP multicast VLAN and IP address, use the **mvr** interface configuration command on the switch stack or on a standalone switch. Use the **no** form of this command to return to the default settings.

mvr [**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* **group** [*ip-address*]]

no mvr [**immediate** | **type** {**source** | **receiver**}| **vlan** *vlan-id* **group** [*ip-address*]]

Syntax Description

immediate	(Optional) Enables the Immediate Leave feature of MVR on a port. Use the **no mvr immediate** command to disable the feature.
type	(Optional) Configures the port as an MVR receiver port or a source port. The default port type is neither an MVR source nor a receiver port. The **no mvr type** command resets the port as neither a source or a receiver port.
receiver	Configures the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN.
source	Configures the port as an uplink port that can send and receive multicast data for the configured multicast groups. All source ports on a switch belong to a single multicast VLAN.
vlan *vlan-id* **group**	(Optional) Adds the port as a static member of the multicast group with the specified VLAN ID. The **no mvr vlan** *vlan-id* **group** command removes a port on a VLAN from membership in an IP multicast address group.
ip-address	(Optional) Statically configures the specified MVR IP multicast group address for the specified multicast VLAN ID. This is the IP address of the multicast group that the port is joining.

Defaults

A port is configured as neither a receiver nor a source.

The Immediate Leave feature is disabled on all ports.

No receiver port is a member of any configured multicast group.

Command Modes

Interface configuration

Command History

Release	Modification
15.0(1)SY	This command was introduced.

Usage Guidelines

Configure a port as a source port if that port should be able to both send and receive multicast data bound for the configured multicast groups. Multicast data is received on all ports configured as source ports.

Receiver ports cannot be trunk ports. Receiver ports on a switch can be in different VLANs, but should not belong to the multicast VLAN.

A port that is not taking part in MVR should not be configured as an MVR receiver port or a source port. A non-MVR port is a normal switch port, able to send and receive multicast data with normal switch behavior.

When Immediate Leave is enabled, a receiver port leaves a multicast group more quickly. Without Immediate Leave, when the switch receives an IGMP leave message from a group on a receiver port, it sends out an IGMP MAC-based query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP MAC-based query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency.

The Immediate Leave feature should be enabled only on receiver ports to which a single receiver device is connected.

The **mvr vlan group** command statically configures ports to receive multicast traffic sent to the IP multicast address. A port statically configured as a member of group remains a member of the group until statically removed. In compatible mode, this command applies only to receiver ports; in dynamic mode, it can also apply to source ports. Receiver ports can also dynamically join multicast groups by using IGMP join messages.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

An MVR port cannot be a private-VLAN port.

Examples

This example shows how to configure a port as an MVR receiver port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr type receiver
```

Use the **show mvr interface** privileged EXEC command to display configured receiver ports and source ports.

This example shows how to enable Immediate Leave on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr immediate
```

This example shows how to add a port on VLAN 1 as a static member of IP multicast group 228.1.23.4:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

You can verify your settings by entering the **show mvr members** privileged EXEC command.

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
show mvr	Displays MVR global parameters or port parameters.
show mvr interface	Displays the configured MVR interfaces or displays the multicast groups to which a receiver port belongs. Also displays all MVR groups of which the interface is a member.
show mvr members	Displays all receiver ports that are members of an MVR multicast group.

platform cts

To configure Cisco Trusted Security (CTS) platform commands, use the **platform cts** command in Global configuration mode. To disable this capability, use the no form of this command.

platform cts {**egress** | **ingress**}

no platform cts {**egress** | **ingress**}

Syntax Description

egress	Configures egress platform packets.
ingress	Configures ingress platform packets.

Command Default

None

Command Modes

Global configuration (config) mode

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

The following example shows how to configure capturing CTS platform packets on the egress:

```
Router (onfig)# platform cts egress
```

The following example shows how to configure capturing CTS platform packets on the ingress:

```
Router# platform cts ingress
```

Related Commands

Command	Description
show platform cts reflector interface	Displays the CTS platform information.

platform hardware cef maximum-routes

To limit the maximum number of the routes that can be programmed in the hardware allowed per protocol, use the **platform hardware cef maximum-routes** command in global configuration mode. To return to the default settings, use the **no** form of this command.

platform hardware cef maximum-routes {**eom-v4-mcast | eom-v6-mcast | eompls | ip | ip-multicast | ipv6 | ipv6-multicast | mpls**} *maximum-routes*

no platform hardware cef maximum-routes {**ip | ip-multicast | ipv6 | mpls**}

Syntax Description

eom-v4-mcast	Specifies the maximum number of eom-v4-mcast routes.
eom-v6-mcast	Specifies the maximum number of eom-v6-mcast routes.
eompls	Specifies the maximum number of EoMPLS routes.
ip	Specifies the maximum number of IP routes.
ip-multicast	Specifies the maximum number of IP multicast routes.
ipv6	Specifies the maximum number of IPv6 routes.
ipv6-multicast	Specifies the maximum number of IPv6 multicast routes.
mpls	Specifies the maximum number of Multiprotocol Label Switching (MPLS) labels.
maximum-routes	Maximum number of the routes that can be programmed in the hardware allowed per protocol.

Command Default

Each protocol has a default maximum route setup of 1000 hardware entries. Each protocol is allowed to use the maximum routes from the shared area.

The defaults for the shared area are as follows:

- For XL-mode systems—512,000 routes
- For non-XL mode systems—248,000 routes

The maximum routes value is based on hardware entries. Different protocols use different numbers of hardware (hw) entries per route:

- IPv4 and MPLS—1 hw entry
- IPv6, IPv4 multicast and Eom-v4 multicast—2 hw entries
- IPv6 multicast and Eom-v6 multicast—4 hw entries4 hw entries

Note See the “Usage Guidelines” section for information on XL and non-XL mode systems.

Command Modes

Global configuration

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

Note If you copy a configuration file that contains the multilayer switching (MLS) Cisco Express Forwarding maximum routes into the startup-config file and reload the Cisco 7600 series router, the Cisco 7600 series router reloads after it reboots.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

System reboot is not required for the maximum routes to take effect. A newly configured maximum route value is validated against the current usage of the hardware FIB. Once validated the new value takes effect immediately.

The maximum routes value for each protocol is configured separately. The new protocols supported include IPv4, IPv4 multicast, IPv6, IPv6 multicast, MPLS, EoMPLS, vpls-v4-multicast, and vpls-v6-multicast. MPLS-VPN routes are counted with MPLS maximum routes setup.

Note Due to limited space usage, diags protocol entries are counted against IPv4-allocated maximum routes value.

The concept of a flexible setting of maximum routes value has been introduced. In addition to a specific maximum routes value per protocol, a single shared area is also defined. This shared area can be used by selected protocols once their dedicated spaces are exhausted.

Combined with the flexible setting feature, the maximum routes value can be used to specify both the minimum and the maximum values of entries to be allocated to a protocol. You can specify whether the protocol is allowed to use the shared area or not.

The **platform cef maximum-routes** command limits the maximum number of the routes that can be programmed in the hardware. If routes are detected that exceed the limit for that protocol, an exception condition is generated.

The determination of XL and non-XL mode is based on the type of Policy Feature Card (PFC) or Distributed Forwarding Card (DFC) modules that are installed in your system. For additional information on systems running Cisco IOS Release 12.2SXF and earlier releases see:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#Policy_Feature_Card_Guidelines_and_Restrictions

For additional information on systems running Cisco IOS Release 12.2SXH and later releases see:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html#Policy_Feature_Card_Guidelines_and_Restrictions

The valid values for the *maximum-routes* argument depend on the system mode—XL mode or non-XL mode. The valid values are as follows:

- XL mode
  - IP and MPLS—Up to 1,007,000 routes
  - IP multicast and IPv6—Up to 503,000 routes
- Non-XL mode
  - IP and MPLS—Up to 239,000 routes
  - IP multicast and IPv6—Up to 119,000 routes

Note The maximum values that you are permitted to configure is not fixed but varies depending on the values that are allocated for other protocols.

An example of how to enter the maximum routes argument is as follows:

```
platform cef maximum-routes ip 4
```

where 4 is 4096 IP routes (1024 x4 = 4096).

The new configurations are applied after a system reload only and do not take effect if a switchover occurs.

In RPR mode, if you change and save the maximum-routes configuration, the redundant supervisor engine reloads when it becomes active from either a switchover or a system reload. The reload occurs 5 minutes after the supervisor engine becomes active.

Use the **show platform cef maximum-routes** command to display the current maximum routes system configuration.

Examples

This example shows how to set the maximum number of routes that are allowed per protocol:

```
Router(config)# platform hardware cef maximum-routes ip 100
```

This example shows how to return to the default setting for a specific protocol:

```
Router(config)# no platform hardware cef maximum-routes ip
```

Related Commands

Command	Description
show platform cef maximum-routes	Displays the current maximum-route system configuration.

platform cts

To enable Cisco Trusted Security (CTS) in egress or ingress mode, use the **platform cts** command.

platform cts {**egress** | **ingress**}

Syntax Description

egress	Specifies the platform hardware CTS egress.
ingress	Specifies the platform hardware CTS ingress.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to enable the CTS in egress mode:

```
Router(config)# platform cts egress
```

Related Commands

Command	Description
show platform cts	Displays the CTS information for the hardware platform.

platform feature-manager

To configure the platform-specific feature manager, use the **platform feature-manager** command.

platform feature-manager {**acl** {**downloadable** {**setup** {**static**}}} | **consistency-check**}

Syntax Description

acl	Specifies the ACL.
downloadable	Specifies downloadable ACLs in operation.
setup	Specifies the setup option for downloadable ACLs.
static	Specifies the static region setup in TCAM for downloadable ACLs.
consistency-check	Specifies consistency checks between the feature manager and other hardware modules.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to configure static region setup in TCAM for downloadable ACLs:

```
Router(config)# platform feature-manager acl downloadable setup static
```

Related Commands

Command	Description
show platform feature-manager	Displays the platform-specific feature manager configuration.

platform feature-manager capture rate-limit

To set the performance capture rate limits of OAL, VACL, Capture, IPv6, Copy, and VM, use the **platform feature-manager capture rate-limit** command in Privileged EXEC mode. To disable performance monitoring, use the **no** form of this command.

platform performance-monitor rate-limit *pps*

no platform performance-monitor rate-limit *pps*

Syntax Description

pps	Specifies the rate limit in packets per second; valid values are 0 through 1000000 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

The following example shows how to set the rate-limit capture to 10000 seconds:

```
Router # platform feature-manager capture rate-limit pps 10000
```

Related Commands

Command	Description
show fm	Displays information about feature manager.

platform hardware acl

To configure the platform hardware ACL statistics, use the **platform hardware acl** command.

platform hardware acl {**cc** {**enable**} | **default-result** {**bridge** | **deny** | **permit**} | **other-protocols** {**prot1** {*range 1* | *range 7* | *range 8* | *range 4* | *range 2* | *range 5* | *range 6* | *range* 3} | **prot2** {*range 1* | *range 7* | *range 8* | *range 4* | *range 2* | *range 5* | *range 6* | *range* 3} | **prot3** {*range 1* | *range 7* | *range 8* | *range 4* | *range 2* | *range 5* | *range 6* | *range* 3} | **prot4** {*range 1* | *range 7* | *range 8* | *range 4* | *range 2* | *range 5* | *range 6* | *range* 3} | **prot5** {*range 1* | *range 7* | *range 8* | *range 4* | *range 2* | *range 5* | *range 6* | *range* 3} | **prot6** {*range 1* | *range 7* | *range 8* | *range 4* | *range 2* | *range 5* | *range 6* | *range* 3}} | **reserve** {**qos-banks** {*num*}| **rbacl-tcam-percentage** {**sgt-dgt** {*percentage*}}} | **update-mode hitless** | **downloadable setup static**}

Syntax Description

cc	Specifies the consistency checker.
enable	Enables consistency checker.
default-result	Specifies the default result to be used during TCAM programming.
bridge	Specifies the bridge result.
deny	Specifies the deny result.
permit	Specifies the permit result.
other-protocols	Specifies the match and classify layer 4 protocol.
prot1	Sets the first protocol.
prot2	Sets the second protocol.
prot3	Sets the third protocol.
prot4	Sets the fourth protocol.
prot5	Sets the fifth protocol.
prot6	Sets the sixth protocol.
range 1	Specifies the Layer 4 protocol range 1. Range is 0–0.
range 2	Specifies the Layer 4 protocol range 2. Range is 3–5.
range 3	Specifies the Layer 4 protocol range 3. Range is 7–16.
range 4	Specifies the Layer 4 protocol range 4. Range is 18–49.
range 5	Specifies the Layer 4 protocol range 5. Range is 51–57.
range 6	Specifies the Layer 4 protocol range 6. Range is 59–102.
range 7	Specifies the Layer 4 protocol range 7. Range is 103–331.
range 8	Specifies the Layer 4 protocol range 8. Range is 133–255.
reserve	Specifies the reserve TCAM.
qos-banks *num*	Specifies the reserve banks for QoS; valid values are 1 or 2.
rbacl-tcam-percentage	Specifies the percent TCAM entries to be reserved for RBACL (egress).
sgt-dgt *percentage*	Specifies the percentage to reserve TCAM for sgt-dgt. Range is 1–98
update-mode hitless	Specifies the hitless TCAM update mode.
downloadable setup static	Disables sharing evaluation when the port is dynamically configured by the authentication server response. The static sharing evaluation may adversely affect the port/host linkup time.

Defaults

Release 15.0(1)SY no payload encryption (NPE) images do not support the hitless ACL update feature or the [**no**] **platform hardware acl update-mode hitless** command.

Release 15.0(1)SY1 and later no payload encryption (NPE) images support hitless ACL update and the **platform hardware acl update-mode hitless** command is configured by default.

In other releases and images, the **platform hardware acl update-mode hitless** command is configured by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.
15.0(2)SY	Support for the **qos-banks** keyword was added.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to configure the paltform hardware ACL protocol 6 with value 105:

```
Router(config)# platform hardware acl other-protocols prot6 105
```

Related Commands

Command	Description
show platform hardware acl	Displays platform hardware ACL statistics.

platform hardware cef

To enable CEF on the hardware platform, use the **platform hardware cef** command.

platform hardware cef {**maximum-routes** {**eom-v4-mcast** *number* | **eom-v6-mcast** *number* | **eompls** *number* | **ip** *number* | **ip-multicast** *number* | **ipv6** *number* | **ipv6-multicast** *number* | **mpls** *number*} | **tunnel** {**fragment**}}

Syntax Description

maximum-routes	Specifies a per-protocol maximum routes configuration.
eom-v4-mcast	Specifies EoM v4 multicast entries; each route takes two entries.
eom-v6-mcast	Specifies EoM v6 multicast entries; each route takes four entries.
eompls	Specifies EoMPLS entries; each route takes one entry.
ip	Specifies IP entries; each route takes one entry.
ip-multicast	Specifies IP-multicast entries; each route takes two entries.
ipv6	Specifies IPv6 entries; each route takes two entries.
ipv6-multicast	Specifies IPv6 multicast entries; each route takes four entries.
mpls	Specifies MPLS entries; each label takes one entry.
number	Specifies the number of 1 K entries. Range is 1–249.
tunnel	Specifies the platform tunnel capabilities.
fragment	Enables tunnel fragmentation on the platform.

Defaults

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to enable CEF with a per-protocol maximum routes configuration using IPv6 for five entries:

```
Router(config)# platform hardware cef maximum-routes ipv6 5
```

Related Commands

Command	Description
show platform hardware cef	Displays the enabled platform hardware CEF information.

platform hardware vsl

To enable VSL on the hardware platform, use the **platform hardware vsl** command.

platform hardware vsl {**pfc** {**mode** {**non-xl**}}}

Syntax Description

pfc	Specifies PFC configuration.
mode	Specifies PFC as the mode.
non-xl	Specifies booting the virtual switch in non-XL mode.

Defaults

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to boot the virtual switch in non-XL mode:

```
Router(config)# platform hardware vsl pfc mode non-xl
```

platform ip

To enable multilayer switching (MLS) IP for the internal router on the interface, use the **platform ip** command in interface configuration mode. To disable MLS IP on the interface use the **no** form of this command.

platform ip

no platform ip

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to enable MLS IP:

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

Related Commands

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

platform ip cef accounting per-prefix

To enable multilayer switching (MLS) per-prefix accounting, use the **platform ip cef accounting per-prefix** command in global configuration mode. To disable MLS per-prefix accounting, use the **no** form of this command

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

no platform ip cef accounting per-prefix

Syntax Description

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

Command Default

MLS per-prefix accounting is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

Command	Description
show platform cef ip	Displays all the prefixes that are configured for the statistic collection.

platform ip cef load-sharing

To configure the Cisco Express Forwarding (CEF) load balancing, use the **platform ip cef load-sharing** command in global configuration mode. To return to the default settings, use the **no** form of this command.

platform ip cef load-sharing [**dst-only**] [**full**] [**ip-only**]

no platform ip cef load-sharing

Syntax Description

dst-only	(Optional) Sets the load-balancing algorithm to include destination to include destination Layer 4 ports and destination IP addresses (Layer 3)
full	(Optional) Sets the Cisco Express Forwarding load-balancing to include source and destination Layer 4 ports and source and destination IP addresses (Layer 3).
ip-only	(Optional) Sets the load-balancing algorithm to include source and destination IP addresses.

Command Default

Source and destination IP address and universal identification

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

The **platform ip cef load-sharing** command affects the IPv4, the IPv6, and the Multiprotocol Label Switching (MPLS) forwardings.

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

- **platform ip cef load-sharing full**—Uses Layer 3 and Layer 4 information with multiple adjacencies.

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 with multiple adjacencies:

```
Router(config)# platform ip cef load-sharing
```

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

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

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

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

This example shows how to return to the default setting:

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

Related Commands

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

platform ipv6 cef

To enable the CEF configuration in IPv6, use the **platform ipv6 cef** command.

platform ipv6 cef {**accounting** {**per-prefix** {**X:X:X:X**}}}

Syntax Description

accounting	Enables the MLF CEF accounting.
X:X:X:X	Specifies the IP address.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to enable the MLF CEF accounting in IPv6 configuration:

```
Router(config)# platform ipv6 cef accounting
```

platform mpls gbte

To configure guaranteed bandwidth traffic engineering (GBTE) flow policing and parameters, use the **platform mpls gbte** command.

platform mpls gbte {**burst** *time* | **cir-ratio** *number* | **dscp** *number* | **global-pool**}

Syntax Description

burst *time*	Specifies the burst duration for guaranteed bandwidth TE flows in milliseconds. Range is 100–30000.
cir-ratio *number*	Specifies the policing at the mentioned ratio with regard to CIR. Range is 1–100.
dscp *number*	Specifies the DSCP map for guaranteed bandwidth TE flows. Range is 0–63.
global-pool	Inspect TE flows using resources allocated from global pool.

Defaults

The default for **cir-ratio** *number* is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to inspect the TE flows using resources allocated from global pool:

```
Router(config)# platform mpls gbte global-pool
```

platform multicast routing

To configure the multicast routing configuration replication mode, use the **platform multicast routing replication egress** command.

platform multicast routing replication egress

Syntax Description

routing replication egress	Enables egress replication mode.

Command Default

None (hardware dependent)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to disable egress replication mode:

```
Router(config)# no platform multicast routing replication egress
```

Related Commands

Command	Description
show platform multicast	Displays the multicast information for the platform.

platform multicast snooping

To configure multicast snooping support, use the **platform multicast snooping** command.

platform multicast snooping {**ltl-share** [**across**] | **flood-to-peer**}

Syntax Description

ltl-share	Enables LTL-sharing within VLANs.
across	Enables LTL-sharing across VLANs.
flood-to-peer	Enables multicast snooping support.

Command Default

platform multicast snooping ltl-share: not configured.

platform multicast snooping flood-to-peer: enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.
15.1(1)SY1	Support for the **flood-to-peer** keyword was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to enable LTL-sharing across VLANs in multicast snooping configuration:

```
Router(config)# platform multicast snooping ltl-share across
```

Related Commands

Command	Description
show platform multicast	Displays the multicast information for the platform.

platform qos 10g-only

To enable quality of service (QoS) in 10g-only mode, in which only the supervisor engine's 10-Gigabit Ethernet uplink ports are used, use the **platform qos 10g-only** command in global configuration mode. To allow the use of all uplink ports, including the 1-Gigabit Ethernet ports, use the **no** form of this command.

platform qos 10g-only

no platform qos 10g-only

Syntax Description

This command has no arguments or keywords.

Command Default

All ports are active on the supervisor engine.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

When you enter the **platform qos 10g-only** command, a supervisor engine with both 1-Gigabit and 10-Gigabit Ethernet uplink ports reallocates the interface queue capacity to improve the performance of its 10-Gigabit Ethernet ports. The reallocation is possible only in 10g-only mode, in which the supervisor engine's 1-Gigabit Ethernet ports are not used. In the normal mode, when all supervisor engine ports are active, the queue structure is 2q4t on receive and 1p3q4t on transmit. In 10g-only mode, the queue structure is 8q4t on receive and 1p7q4t on transmit.

Note To display detailed information about the queues, use the **show queueing interface** command.

When you switch between normal and 10g-only modes, any existing QoS configuration on the uplink ports is lost, and you must reconfigure QoS. In addition, service will be temporarily lost on the ports during the transition.

If you do not shut down the 1-Gigabit Ethernet ports before entering the **platform qos 10g-only** command, the **platform qos 10g-only** command shuts down the ports.

When you switch from 10g-only mode to normal mode, you must enter the **no shutdown** command on each of the 1-Gigabit Ethernet ports to resume QoS service on those ports.

In 10g-only mode, the 1-Gigabit Ethernet ports are visible, but they remain in an administratively down state.

The **platform qos 10g-only** command affects only active and standby supervisors, but if you have four supervisors you must apply it to the in-chassis standby supervisors.

Examples

The following example shows how to place the supervisor engine in the 10g-only mode:

```
Router# configure terminal
Router(config)# platform qos 10g-only
```

Related Commands

Command	Description
show platform qos interface	Displays QoS information.

platform qos aggregate-policer

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

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

no platform 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 the *normal-burst-bytes value*).
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 committed information rate (cir) rate.

action-type action	(Optional) Action type. This argument can include multiple action types and corresponding actions to set several actions simultaneously. The following are valid values: • **conform-action**—Specifies the action to be taken when the rate is not exceeded. Valid actions are as follows: – **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**—Specifies the action to be taken when QoS values are exceeded. Valid actions are as follows: – **drop**—Drops the packet. This is the default. – **policed-dscp-transmit**—Changes the DSCP value according to the *policed-dscp map* value and sends the packet. – **transmit**—Transmits the packet. • **violate-action**—Specifies the action to be taken when QoS values are violated. Valid actions are as follows: – **drop**—Drops the packet. – **policed-dscp-transmit**—Changes the DSCP value according to the *policed-dscp map* value and sends the packet. – **transmit**—Transmits the packet.

Command Default

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 (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

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 **platform 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). If you modify an existing aggregate rate limit entry, that entry is 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.

When you enter the aggregate policer name, follow these naming conventions:

- Can be a maximum of 31 characters and can include a to z, A to Z, 0 to 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.
- 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 platform 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)# platform qos aggregate-policer micro-one 100000 10000 conform-action
set-dscp-transmit 48 exceed-action drop
```

Related Commands

Command	Description
police (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 platform qos aggregate policer	Displays information about the aggregate policer for MLS QoS.

platform qos marking statistics

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

platform qos marking statistics

no platform qos marking statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

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

Examples

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

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

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

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

Related Commands

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

platform qos protocol

To define routing-protocol packet policing, use the **platform qos protocol** command in global configuration mode. To return to the default settings, use the **no** form of this command.

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

no platform qos protocol *protocol-name*

Syntax Description

protocol-name	Protocol name. Valid values include the following: • **arp** • **bfd-ctrl** • **bfd-echo** • **bgp** • **eigrp** • **glbp** • **igrp** • **isis** • **ldp** • **nd** • **ospf** • **rip** • **vrrp**
pass-through	Specifies the pass-through mode.
police *rate*	Specifies the maximum bits per second (bps) to be policed. Valid values are from 32000 to 4000000000.
burst	(Optional) Normal burst bytes. Valid values are from 1000 to 31250000.
precedence *value*	Specifies the IP-precedence value of the protocol packets to rewrite. Valid values are from 0 to 7.

Command Default

The defaults are as follows:

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

This command does not support ARP, ISIS, or EIGRP on Cisco 7600 series routers or Catalyst 6500 switches that are configured with a Supervisor Engine 2.

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

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

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

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

You can make the protocol packets avoid policing completely if you choose the pass-through mode. If the police mode is chosen, the committed information rate (CIR) specified is the rate that is used to police all the specified protocol's packets, both entering or leaving the Cisco 7600 series router.

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

Examples

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

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

This example shows how to avoid policing completely:

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

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

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

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

```
Router(config)# platform qos protocol bgp precedence 4 police 32000 1200
```

Related Commands

Command	Description
show platform qos protocol	Displays protocol pass-through information.

platform qos rewrite ip dscp

To enable type of service (ToS)-to-differentiated services code point (DSCP) rewrite, use the **platform qos rewrite ip dscp** command in global configuration mode. To disable ToS-to-DSCP rewrite, use the **no** form of this command.

platform qos rewrite ip dscp [**slot** *slot1*,*slot2*,*slot3*...]

no platform qos rewrite ip dscp [**slot** *slot1*,*slot2*,*slot3*...]

Syntax Description

slot *slot*	(Optional) Specifies the slot number. Use the **platform qos rewrite ip dscp slot ?** command to determine the valid slots for your chassis.

Command Default

ToS-to-DSCP rewrite is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

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

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

The **no platform qos rewrite ip dscp** command is incompatible with Multiprotocol Label Switching (MPLS). The default **platform qos rewrite ip dscp** command must remain enabled in order for the PFC3BXL or PFC3B to assign the correct MPLS Experimental (EXP) value for the labels that it imposes. This restriction does not apply to PFC3C or PFC3CXL forward.

The **platform qos rewrite ip dscp slot** command can be used for disabling ToS-to-DSCP rewrite on supervisors or DFC line cards. Although the command will be accepted for non-DFC line card slots, it does not come into effect unless a DFC line card is inserted into that slot.

To disable rewrite on packets that are coming in on non-DFC line cards, disable the rewrite on the supervisor slots. Note that this disables the rewrite on packets that are coming in on all non-DFC line cards on the system.

Examples

The following example shows how to enable ToS-to-DSCP rewrite in slot 4:

```
Router(config)# platform qos rewrite ip dscp slot 4
```

The following example shows how to disable port-queueing mode globally:

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

Related Commands

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

platform qos statistics-export delimiter

To set the quality of service (QoS) statistics data export field delimiter, use the **platform qos statistics-export delimiter** command in global configuration mode. To return to the default settings, use the **no** form of this command.

platform qos statistics-export delimiter

no platform qos statistics-export delimiter

Syntax Description

This command has no arguments or keywords.

Command Default

The default delimiter is the pipe character (|).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

QoS statistics data export is not supported on Optical Service Module (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)# platform qos statistics-export delimiter ,
```

Related Commands

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

platform qos statistics-export destination

To configure the quality of service (QoS) statistics data export destination host and User Datagram Protocol (UDP) port number, use the **platform qos statistics-export destination** command in global configuration mode. To return to the default settings, use the **no** form of this command.

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

no platform 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; see the "Usage Guidelines" section for a list of valid values.
severity *severity-value*	(Optional) Specifies the severity level to export; see the "Usage Guidelines" section for a list of valid values.

Command Default

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

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

QoS statistics data export is not supported on Optical Service Module (OSM) interfaces.

Valid *facility* values are as follows:

- **authorization**—Security and authorization messages
- **cron**—Clock daemon
- **daemon**—System daemon
- **kernel**—Kernel messages

- **local0**—Local use 0
- **local1**—Local use 1
- **local2**—Local use 2
- **local3**—Local use 3
- **local4**—Local use 4
- **local5**—Local use 5
- **local6**—Local use 6
- **local7**—Local use 7
- **lpr**—Line printer subsystem
- **mail**—Mail system
- **news**—Network news subsystem
- **syslog**—Messages that are generated internally by syslog
- **user**—User-level messages
- **uucp**—UNIX-to-UNIX Copy Program (UUCP) subsystem

Valid *severity* levels are as follows:

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

Examples

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

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

Related Commands

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

platform qos statistics-export interval

To specify how often a port or aggregate-policer quality of service (QoS) statistics data is read and exported, use the **platform qos statistics-export interval** command in global configuration mode. To return to the default settings, use the **no** form of this command.

platform qos statistics-export interval *interval*

no platform qos statistics-export interval

Syntax Description

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

Command Default

300 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

QoS statistics data export is not supported on Optical Services Module (OSM) interfaces.

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

Caution Be careful when decreasing the interval because exporting QoS statistics imposes a significant load on the Cisco 7600 series router.

Examples

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

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

Related Commands

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

platform rate-limit all

To enable and set the rate limiters that are common to unicast and multicast packets in the global configuration command mode, use the **platform rate-limit all** command. Use the **no** form of this command to disable the rate limiters.

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

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

Syntax Description

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

Defaults

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

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

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

Related Commands

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

platform rate-limit layer2

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

platform rate-limit layer2 {**ip-admission** | **l2pt** | **pdu** | **port-security**| **unknown**} *pps* [*packets-in-burst*]

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

Syntax Description

ip-admission *pps*	Specifies the rate limit for IP admission on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
l2pt *pps*	Specifies the rate limit for control packets in Layer 2 with a protocol-tunneling multicast-MAC address in Layer 2; valid values are from 10 to 1000000 packets per second.
pdu *pps*	Specifies the rate limit for Bridge Protocol Data Unit (BPDU), Cisco Discovery Protocol (CDP), Protocol Data Unit (PDU), and VLAN Trunk Protocol (VTP) PDU Layer 2 control packets; valid values are from 10 to 1000000 packets per second.
port-security *pps*	Specifies the rate limit for port security traffic; valid values are from 10 to 1000000 packets per second.
unknown *pps*	Specifies the rate limit for unknown unicast flooding on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

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

```
Router(config)# platform rate-limit layer2 pdu pkt 100 burst 100
```

Related Commands

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

platform rate-limit multicast

To configure the platform rate-limits for multicasts, use the **platform rate-limit multicast** command.

platform rate-limit multicast {**flood** {**byte** *rate* | **pkt** *rate*} | **flood-ip** {**byte** *rate* | **pkt** *rate*} | **flood-ip-control** {**byte** *rate* | **pkt** *rate*} | **ipv4** {**connected** {**byte** *rate* | **pkt** *rate*} | **ipv6** {**connected** {**byte** *rate* | **pkt** *rate*} }

Syntax Description

flood	Specifies all multicast flooded frames.
byte *rate*	Specifies the byte rate. Range is 0–4294967295.
pkt *rate*	Specifies the packet rate. Range is 0–33554431.
flood-ip	Specifies all IP multicast flooded frames.
flood-ip-control	Specifies IP multicast flooded control frames.
ipv4	Specifies IPv4 multicast rate limiters.
ipv6	Specifies IPv6 multicast rate limiters.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows how to configure the platform rate-limit multicast flood:

```
Router(config)# platform rate-limit multicast flood pkt 100 burst 100
```

Related Commands

Command	Description
show platform rate-limit multicast	Displays the platform rate limits for multicasts.

platform rate-limit multicast ipv4

To enable and set the rate limiters for the IPv4 multicast packets in the global configuration command mode, use the **platform rate-limit multicast ipv4** command. Use the **no** form of this command to disable the rate limiters.

platform rate-limit multicast ipv4 {**connected** | **fib-miss** | **igmp** | **ip-option** | **pim**} *pps* [*packets-in-burst*]

no platform rate-limit multicast ipv4 {**connected** | **fib-miss** | **igmp** | **ip-option** | **pim**}

Syntax Description

connected	Enables and sets the rate limiters for multicast packets from directly connected sources.
fib-miss	Enables and sets the rate limiters for the FIB-missed multicast packets.
igmp	Enables and sets the rate limiters for the IGMP packets.
ip-option	Enables and sets the rate limiters for the multicast packets with IP options.
pim	Enables and sets the rate limiters for the multicast packets with PIM options.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

This example shows how to set the rate limiters for the multicast packets from directly connected sources:

```
Router(config)# platform rate-limit multicast ipv4 connected pkt 100 burst 100
Router(config)#
```

Related Commands

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

platform rate-limit multicast ipv6

To configure the IPv6 multicast rate limiters, use the **platform rate-limit multicast ipv6** command in global configuration mode. To disable the rate limiters, use the **no** form of this command.

platform rate-limit multicast ipv6 {**connected** *pps* [*packets-in-burst*] | **control-packet** | **mld**}

no platform rate-limit multicast ipv6 {**connected** *pps* [*packets-in-burst*] | **control-packet** | **mld**}

Syntax Description

connected *pps*	Enables and sets the rate limiters for the IPv6 multicast packets from a directly connected source; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
control-packet	Enables and sets the rate limiters for the IPv6 multicast control packets
mld	Enables and sets the rate limiters for the IPv6 multicast MLD packets

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

This example shows how to set the rate limiters for the IPv6 multicast packets from a directly connected source:

```
Router(config)#platform rate-limit multicast ipv6 connected pkt 100 burst 100
Router(config)#
```

Related Commands

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

platform rate-limit unicast acl

To enable and set the ACL-bridged rate limiters in global configuration command mode, use the **platform rate-limit unicast acl** command. Use the **no** form of this command to disable the rate limiters.

platform rate-limit unicast acl {**input | mac-pbf | output | vacl-log**} *pps* [*packets-in-burst*]

no platform rate-limit unicast acl {**input | mac-pbf | output | vacl-log**} *pps* [*packets-in-burst*]

Syntax Description

input	Specifies the rate limiters for the input ACL-bridged unicast packets.
mac-pbf	Specifies the rate limiters for the MAC PBF.
output	Specifies the rate limiters for the output ACL-bridged unicast packets.
vacl-log	Specifies the rate limiters for the VACL log cases.
pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- **input**—Disabled.
- **output**—Disabled.
- **vacl-log**—Enabled at **2000** *pps* and *packets-in-burst* value is set to **1**.
- If the *packets-in-burst* value is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group 1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode.

Examples

This example shows how to set the input ACL-bridged packet limiter for unicast packets:

```
Router(config)# platform rate-limit unicast acl input pkt 100 burst 100
Router(config)#
```

Related Commands

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

platform rate-limit unicast cef

To enable and set the Cisco Express Forwarding (CEF) rate limiters in global configuration command mode, use the **platform rate-limit unicast cef** command. Use the **no** form of this command to disable the rate limiters.

platform rate-limit unicast cef {**receive** | **glean**}{**byte byte_per_second** [**bytes_allowed_in_each_burst**] | **pkt pkt_per_second** [**packets_allowed_in_each_burst**]} {**burst burst_period_in_microsecond**} [**leak**]

no platform rate-limit unicast cef {**receive** | **glean**}{**byte byte_per_second** [**bytes_allowed_in_each_burst**] | **pkt pkt_per_second** [**packets_allowed_in_each_burst**]} {**burst burst_period_in_microsecond**} [**leak**]

Syntax Description

receive	Enables and sets the rate limiters for receive packets.
glean	Enables and sets the rate limiters for ARP-resolution packets.
pps	Packets per second; valid values are from 0 to 33554431 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- **glean** pkt_per_second = 1000 burst_period_in_microsecond = 1000000
- **vacl-log** pkt_per_second = 100 burst_period_in_microsecond = 1000000

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Examples

This example shows how to set the CEF-glean limiter for the unicast packets:

```
Router(config)# platform rate-limit unicast cef glean 5000
Router(config)#
```

Related Commands

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

platform rate-limit unicast ip

To enable and set the rate limiters for the unicast packets in global configuration command mode, use the **platform rate-limit unicast ip** command. Use the **no** form of this command to disable the rate limiters.

platform rate-limit unicast ip {**arp-inspection** | **dhcp-snooping** | **errors** | **features** | **options** | **rpf-failure**} *pps* [*packets-in-burst*]

platform rate-limit unicast ip icmp {**redirect** | **unreachable acl-drop** *pps* | **no-route** *pps*} [*packets-in-burst*]

no platform rate-limit unicast ip {**errors** | **features** | **icmp** {**redirect** | **unreachable** {**acl-drop** | **no-route**}} | **options** | **rpf-failure**} *pps* [*packets-in-burst*]

Syntax Description

arp-inspection	Specifies rate limiting for unicast packets with dynamic ARP inspection.
dhcp-snooping	Specifies rate limiting for unicast packets with DHCP snooping.
errors	Specifies rate limiting for unicast packets with IP checksum and length errors.
features	Specifies rate limiting for unicast packets with software-security features in Layer 3 (for example, authorization proxy, IPsec, and inspection).
options	Specifies rate limiting for unicast IPv4 packets with options.
rpf-failure	Specifies rate limiting for unicast packets with RPF failures.
pps	Packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
icmp redirect	Specifies rate limiting for unicast packets requiring ICMP redirect.
icmp unreachable acl-drop *pps*	Enables and sets the rate limiters for the ICMP unreachables for the ACL-dropped packets.
icmp unreachable no-route *pps*	Enables and sets the rate limiters for the ICMP unreachables for the FIB-miss packets.

Command Default

The defaults are as follows:

- If the *packets-in-burst* value is not set, a default of **10** is programmed as the burst for unicast cases.
- **errors**—Enabled at **100** *pps* and *packets-in-burst* value is set to **10**.
- **rpf-failure**—Enabled at **100** *pps* and *packets-in-burst* value is set to **10**.
- **icmp unreachable acl-drop**—Enabled at **100** *pps* and *packets-in-burst* value is set to **10**.
- **icmp unreachable no-route**—Enabled at **100** *pps* and *packets-in-burst* value is set to **10**.
- **icmp redirect**—Disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Note When you configure an ICMP rate limiter, and an ICMP redirect occurs, exiting data traffic is dropped while the remaining traffic on the same interface is forwarded.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group 1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - IP options
  - ICMP unreachable for ACL drop

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode.

Examples

This example shows how to set the ICMP-redirect limiter for unicast packets:

```
Router(config)# platform rate-limit unicast ip option pkt 100 burst 100
Router(config)#
```

Related Commands

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

platform redundancy bias

To configure platform redundancy boot bias, use the **platform redundancy bias** command.

platform redundancy bias *milliseconds*

Syntax Description

bias *milliseconds*	Specifies the platform redundancy bias time in milliseconds. Range is 11–3600.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	Support for this command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

This example shows the platform redundancy bias time in 20 milliseconds:

```
Router(config)# platform redundancy bias 20
```

Related Commands

Command	Description
show platform redundancy	Displays the platform redundancy bias time set in milliseconds.