

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.
<i>mac-address</i>	(Optional) Specifies the MAC address.
interface	(Optional) Clears all addresses for an interface.
<i>type</i>	(Optional) Interface type: ethernet, fastethernet, fddi, atm, or port channel.
<i>slot</i>	(Optional) Module interface number.
<i>interface-type</i> <i>interface-number</i>	(Optional) Module and port number. See the “Usage Guidelines” section for valid values.
notification mac-move counter	Clears the MAC-move notification counters.
<i>vlan</i>	(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 <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

<i>module</i>	(Optional) The module interface number: <ul style="list-style-type: none"> • 0 for fixed • 1 or A for module A • 2 or B for module B
<i>port</i>	(Optional) Port interface number ranging from 1 to 28: <ul style="list-style-type: none"> • 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 <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface number. Range is 1–6.
async <i>number</i>	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 <i>number</i>	Specifies the loopback interface number. Range is 1–2147483647.
mfr <i>number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink <i>number</i>	Specifies the multilink group interface number. Range is 1–2147483647.
null <i>number</i>	Specifies the null interface number. Range is 0–0.
port-channel <i>number</i>	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup <i>number</i>	Specifies the port group interface number. Range is 1–6.
pos-channel <i>number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom bus clock controller interface number. Range is 1–6.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.
virtual-tokenring <i>number</i>	Specifies the virtual Token Ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the Fibre Channel interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	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 <i>number</i>	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	Parameter	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}
```

Syntax	Description
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	<p>This example shows how to clear the platform hardware statistics for module 4:</p> <pre>Router# clear platform hardware statistics module 4</pre>
-----------------	--

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.
<i>interface-type</i>	(Optional)	Interface type. Possible valid values are ethernet , fastethernet , gigabitethernet , and tengigabitethernet . See the “Usage Guidelines” section for additional valid values.
<i>interface-number</i>	(Optional)	Module and port number. See the “Usage Guidelines” section for valid values.
null <i>interface-number</i>	(Optional)	Specifies the null interface. The valid value is 0.
port-channel <i>number</i>	(Optional)	Specifies the channel interface. Valid values are a maximum of 64 values ranging from 1 to 256.
vlan <i>vlan-id</i>	(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 software acl accounting-stats** command.

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

Syntax Description	module <i>number</i> 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	<p>This example shows how to clear the platform software ACL accounting statistics for module 4:</p> <pre>Router# clear platform software acl accounting-stats module 4</pre>
-----------------	---

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

source-ip-address	(Optional) Captures all packets matching a source IP address.
srcindex	(Optional) Captures all packets matching a source index; valid values are <i>index-value</i> 0 to 1048575.
vlan <i>vlan-num</i>	(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
- Loopback
- Lspvif
- MFR
- Multilink
- Null
- Port-channel
- Sysclock
- TenGigabitEthernet

- Tunnel
- Vif
- Virtual-Ethernet
- Virtual-Template
- Virtual-TokenRing
- VLAN
- VoabypassIn
- VoabypassOut
- VoafilterIn
- VoafilterOut
- Voain
- Voayout

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		
<i>ipaddr</i>	Captures packets for a specific destination IP address.	
ipv6 <i>ipaddr</i>	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	<i>mac-addr</i> (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	<i>index-value</i> (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	<i>ethertype</i> (Optional) Captures all packets matching an ethertype; ethertype must be entered in hexadecimal 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	<i>interface</i> (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
- Loopback
- 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.
<i>ipaddr</i>	Captures packets for a specific destination IP address.
ipv6 <i>ipaddr</i>	Captures all packets matching the IPv6 destination IP address.
dmac <i>mac-addr</i>	(Optional) Captures packets matching a destination MAC address index.
dstindex <i>index-value</i>	(Optional) Captures all packets matching a destination index; valid values are 0 to 1048575.
ethertype <i>ethertype</i>	(Optional) Captures all packets matching an ethertype; ethertype must be entered in hexadecimal format.
interface <i>interface</i>	(Optional) Captures packets related to the interface. See Usage Guidelines.
smac <i>smac</i>	(Optional) Captures packets matching the source MAC address; smac must be entered in hexadecimal format.
source-ip-address	(Optional) Captures all packets matching a source IP address.
srcindex <i>index-value</i>	(Optional) Captures all packets matching a source index; valid values are 0 to 1048575.
vlan <i>vlan-num</i>	(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
- Loopback
- 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	<i>smac</i>	(Optional) Captures packets matching the source MAC address; smac must be entered in hexadecimal 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		
	<i>ipaddr</i>	Captures packets for a specific destination IP address.
	ipv6 <i>ipaddr</i>	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	<i>index-value</i> (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.
<i>ipaddr</i>	Captures packets for a specific destination IP address.
ipv6 <i>ipaddr</i>	Captures all packets matching the IPv6 destination IP address.
dmac <i>mac-addr</i>	(Optional) Captures packets matching a destination MAC address index.
dstindex <i>index-value</i>	(Optional) Captures all packets matching a destination index; valid values are 0 to 1048575.
ethertype <i>ethertype</i>	(Optional) Captures all packets matching an ethertype; ethertype must be entered in hexadecimal format.
interface <i>interface</i>	(Optional) Captures packets related to the interface. See Usage Guidelines.
or-filter	(Optional) Applies filters.
smac <i>smac</i>	(Optional) Captures packets matching the source MAC address; smac must be entered in hexadecimal format.
source-ip-address	(Optional) Captures all packets matching a source IP address.
srcindex <i>index-value</i>	(Optional) Captures all packets matching a source index; valid values are 0 to 1048575.
vlan <i>vlan-num</i>	(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	<i>vlan-num</i> (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 debugging 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	<i>seconds</i>	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# no 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.
	<i>percentage</i>	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.
<i>discr-name</i>	(Optional) String of a maximum of eight alphanumeric, case-sensitive characters. Blank spaces between characters are not allowed.
<i>buffer-size</i>	(Optional) Size of the buffer, in bytes. The range is 4096 to 2147483647. The default size varies by platform.
<i>severity-level</i>	(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 <i>severity-level</i> 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 <i>discr-name</i> 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	<i>seconds</i>	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 <i>vlan-id</i>	(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 <i>vlan-id</i>	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.
	<i>interface slot/port</i>	Interface type, the slot number, and the port number.
	module <i>num</i>	(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 reenables 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 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:
 - **history 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] }
[dcli dcli | 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] }
[dcli dcli | pvc vpi/vci] [auto-learn | disable-snooping] [protocol {ip | ipx | assigned}]
```

Syntax Description	
<i>mac address</i>	Address to add to the MAC address table.
vlan <i>vlan-id</i>	Specifies the VLAN associated with the MAC address entry. The range is from 2 to 100.
interface <i>int</i>	Specifies the interface type and the slot and port to be configured. The <i>int</i> argument should specify the interface <i>type</i> and the <i>slot/port</i> or <i>slot/subslot/port</i> 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.
dcli <i>dcli</i>	(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 <i>vpi/vci</i>	(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 **dcli** 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 **dcli** 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 dcli 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 <i>seconds</i>	(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 Commands

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 disable the 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

<i>span-session-number</i>	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: <ul style="list-style-type: none"> • 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 <i>erspan-destination-session-number</i> <i>rspan-destination-session-number</i> 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 <i>session-description</i>	(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 { <i>single-interface</i> <i>interface-list</i> <i>interface-range</i> <i>mixed-interface-list</i> }	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 <i>ip-address</i> [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 <i>erspan-flow-id</i>	Configures the ID number used by the destination and destination sessions to identify the ERSPAN traffic.
vrf <i>vrf-name</i>	(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 <i>erspan-source-session-number</i> 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 <i>session-description</i>	(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 { { <i>single-interface</i> <i>interface-list</i> <i>interface-range</i> <i>mixed-interface-list</i> <i>single-vlan</i> <i>vlan-list</i> <i>vlan-range</i> <i>mixed-vlan-list</i> } [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 { <i>single-vlan</i> <i>vlan-list</i> <i>vlan-range</i> <i>mixed-vlan-list</i> }	(Optional) Configures source VLAN filtering when the ERSPAN or RSPAN source is a trunk port.
description <i>session-description</i>	(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 <i>ip-address</i>	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 <i>erspan-flow-id</i>	Configures the ID number used by the source and destination sessions to identify the ERSPAN or RSPAN traffic.
origin ip address <i>ip-address</i>	Configures the IP address used as the source of the ERSPAN or RSPAN traffic.
ip {{ ttl <i>ttl-value</i> } {{ prec <i>ipp-value</i> } {{ dscp <i>dscp-value</i> }}	(Optional) Configures the following packet values in the ERSPAN or RSPAN traffic: <ul style="list-style-type: none"> ttl <i>ttl-value</i>—IP time-to-live (TTL) value prec <i>ipp-value</i>—IP-precedence value dscp <i>dscp-value</i>—IP-precedence value
vrf <i>vrf-name</i>	(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 <i>num</i>	Specifies the SPAN destination analysis-module.
anomaly-detector-module <i>num</i>	Specifies the SPAN destination anomaly-detector-module.
interface <i>type number</i>	Specifies the interface <i>type</i> and <i>number</i> as follows: <ul style="list-style-type: none"> • GigabitEthernet <i>mod/port</i> • port-channel <i>num</i>—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 <i>num</i>	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 <i>type number</i>	Specifies the interface type and number as follows: <ul style="list-style-type: none"> • FastEthernet <i>mod/port</i> • GigabitEthernet <i>mod/port</i> • Port-channel <i>num</i>—Ethernet Channel of interfaces; valid values are from 1 to 496.
vlan <i>vlan-id</i>	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 <i>ip-address</i>	(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.
<i>count</i>	(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 <i>value</i>	(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 <i>vlan-id</i>	(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 <i>vlan-id</i> group	(Optional) Adds the port as a static member of the multicast group with the specified VLAN ID. The no mvr vlan <i>vlan-id</i> group command removes a port on a VLAN from membership in an IP multicast address group.	
<i>ip-address</i>	(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.
<i>maximum-routes</i>	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 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	Parameter	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	<i>pps</i>	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.
<i>range 1</i>	Specifies the Layer 4 protocol range 1. Range is 0–0.
<i>range 2</i>	Specifies the Layer 4 protocol range 2. Range is 3–5.
<i>range 3</i>	Specifies the Layer 4 protocol range 3. Range is 7–16.
<i>range 4</i>	Specifies the Layer 4 protocol range 4. Range is 18–49.
<i>range 5</i>	Specifies the Layer 4 protocol range 5. Range is 51–57.
<i>range 6</i>	Specifies the Layer 4 protocol range 6. Range is 59–102.
<i>range 7</i>	Specifies the Layer 4 protocol range 7. Range is 103–331.
<i>range 8</i>	Specifies the Layer 4 protocol range 8. Range is 133–255.
reserve	Specifies the reserve TCAM.
qos-banks <i>num</i>	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 <i>percentage</i>	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 platform 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.
<i>number</i>	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

<i>prefix-entry</i>	Prefix entry in the format A.B.C.D.
<i>prefix-entry-mask</i>	Prefix entry mask in the format A.B.C.D.
<i>instance-name</i>	(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 <i>time</i>	Specifies the burst duration for guaranteed bandwidth TE flows in milliseconds. Range is 100–30000.
cir-ratio <i>number</i>	Specifies the policing at the mentioned ratio with regard to CIR. Range is 1–100.
dscp <i>number</i>	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

<i>name</i>	Name of the aggregate policer. See the “Usage Guidelines” section for naming conventions.
<i>rate-bps</i>	Maximum bits per second. Range is 32000 to 10000000000.
<i>normal-burst-bytes</i>	(Optional) Normal burst bytes. Range is 1000 to 31250000.
<i>maximum-burst-bytes</i>	(Optional) Maximum burst bytes. Range is 1000 to 31250000 (if entered, this value must be set equal to the <i>normal-burst-bytes</i> value).
pir <i>peak-rate-bps</i>	(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.

<i>action-type action</i>	<p>(Optional) Action type. This argument can include multiple action types and corresponding actions to set several actions simultaneously. The following are valid values:</p> <ul style="list-style-type: none"> • conform-action—Specifies the action to be taken when the rate is not exceeded. Valid actions are as follows: <ul style="list-style-type: none"> – drop—Drops the packet. – set-dscp-transmit <i>value</i>—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 <i>number</i>—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: <ul style="list-style-type: none"> – drop—Drops the packet. This is the default. – policed-dscp-transmit—Changes the DSCP value according to the <i>policed-dscp map</i> 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: <ul style="list-style-type: none"> – drop—Drops the packet. – policed-dscp-transmit—Changes the DSCP value according to the <i>policed-dscp map</i> 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

<i>protocol-name</i>	Protocol name. Valid values include the following: <ul style="list-style-type: none"> • 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.
<i>burst</i>	(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 <i>slot</i>	(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

<i>host-name</i>	Host name.
<i>host-ip-address</i>	Host IP address.
port <i>port-number</i>	Specifies the UDP port number.
syslog	Specifies the syslog port.
facility <i>facility-name</i>	(Optional) Specifies the type of facility to export; see the “Usage Guidelines” section for a list of valid values.
severity <i>severity-value</i>	(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.
	<i>pps</i>	Packets per second; valid values are from 10 to 1000000 packets per second.
	<i>packets-in-burst</i>	(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 <i>pps</i>	Specifies the rate limit for IP admission on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
l2pt <i>pps</i>	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 <i>pps</i>	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 <i>pps</i>	Specifies the rate limit for port security traffic; valid values are from 10 to 1000000 packets per second.
unknown <i>pps</i>	Specifies the rate limit for unknown unicast flooding on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
<i>packets-in-burst</i>	(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	Parameter	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.
<i>pps</i>	Packets per second; valid values are from 10 to 1000000 packets per second.
<i>packets-in-burst</i>	(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 <i>pps</i>	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.	
<i>packets-in-burst</i>	(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.
<i>pps</i>	Packets per second; see the “Usage Guidelines” section for valid values.
<i>packets-in-burst</i>	(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.
<i>pps</i>	Packets per second; valid values are from 0 to 33554431 packets per second.
<i>packets-in-burst</i>	(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.
<i>pps</i>	Packets per second.
<i>packets-in-burst</i>	(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 unreachable for the ACL-dropped packets.
icmp unreachable no-route pps	Enables and sets the rate limiters for the ICMP unreachable 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 <i>milliseconds</i> 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.

platform software

To enable ACL or QoS configuration on the software platform, use the **platform software** command.

```
platform software {acl {log_update {rate-limit-msg {disable | enable}}} | qos {logging
{bootup}}}
```

Syntax Description		
acl		Specifies ACL as the keyword.
log_update		Specifies log updates for the Classification Manager.
rate-limit-msg		Specifies syslog rate limiting.
disable		Disables syslog rate limiting.
enable		Enables syslog rate limiting at one per second.
qos		Specifies QoS as the keyword.
logging		Specifies the logging-related parameters for QoS.
bootup		Enables QoS logging during bootup.

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 syslog rate limiting for ACL:

```
Router(config)# platform software acl log-update rate-limit-msg enable
```

platform software met profile

To configure allocation percentages for each block size of the multicast expansion, use the **platform software met profile** command. To disable allocation percentages, use the **no** form of this command.

platform software met profile { *value* | *value* | *value* | *value* }

Syntax Description

<i>value</i>	Sets the percentage allocation for each block size; valid values are 0 to 100 percent.
--------------	--

Defaults

The default values are 10 30 50 10 for each of the block sizes.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The new profile will take effect on the switch after reload.

You must configure all four of the profile blocks, and the total block percentages cannot exceed 100 percent.

Examples

This example shows how to set the block percentage for 4 blocks:

```
Router# platform software met profile 20 20 10 50
```

Related Commands

Command	Description
debug platform software multicast routing	Displays information about multicast errors.
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.

platform system-controller reset-threshold

To configure the system controller reset threshold, use the **platform system-controller reset-threshold** command.

platform system-controller reset-threshold {*threshold-num*}

Syntax Description	<i>threshold-num</i> Specifies the threshold reset number; valid values are 1 to 100.
---------------------------	---

Defaults	System controller reset is set to 1.
-----------------	--------------------------------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	12.2(33)SX110	Support for this command was introduced.
	12.2(33)SXJ4	Support for this command was introduced.
	15.1(1)SY	Support for this command was introduced.

Usage Guidelines

If you have a redundant supervisor engine and a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, the affected supervisor engine reloads. When you do not have a redundant supervisor engine and a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, one of the following happens:

- If the system controller reset threshold has not been reached, the system controller ASIC resets the supervisor engine and this message is displayed:

```
%SYSTEM_CONTROLLER-<>-THRESHOLD
%SYSTEM_CONTROLLER-<>-ERROR
%SYSTEM_CONTROLLER-<>-MISTRAL_RESET
```

- If the system controller reset threshold has been reached, the supervisor engine reloads and this message is displayed.

```
%SYSTEM_CONTROLLER-<>-ERROR
%SYSTEM_CONTROLLER-<>-FATAL
```

Examples

This example shows how to configure the system controller reset threshold to 55:

```
Router(config)# platform system-controller reset-threshold 55
```

platform verify

To enable Layer 3 error checking in the hardware, use the **platform verify** command in global configuration mode. To disable Layer 3 error checking in the hardware, use the **no** form of this command.

```
platform verify ipv4 {checksum | length {consistent | minimum} | same-address | tiny-frag}
```

```
platform verify ipv6 {length {consistent} | tiny-frag}
```

```
platform verify syslog
```

Syntax Description

checksum	Enables the checksum-error check.
same-address	Enables the packets having same source and destination IP.
length consistent	Enables the length-consistency check in Layer 2.
length minimum	Enables the minimum-length packet check in Layer 2.
tiny-frag	Enables the first TCP tiny fragment.
syslog	Enables the syslog packet parse errors.

Command Default

checksum

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The minimum-length packets are the packets with an IP header length or IP total length field that is smaller than 20 bytes.

When entering the minimum keyword, follow these guidelines:

- When enabling the IP "too short" check using the **platform verify ip length minimum** command, valid IP packets with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.
- When entering the **no platform verify ip length minimum** command, minimum-length packets are hardware switched. The packets that have IP protocol = 6 (TCP) are sent to the software.

Examples

This example shows how to enable Layer 3 error checking in the hardware:

```
Router(config)# platform verify ip checksum
```

```
Router(config)#
```

This example shows how to disable Layer 3 error checking in the hardware:

```
Router(config)# no platform verify ip checksum
```

```
Router(config)#
```

platform xconnect l2gre tunnel

To configure the Layer 2 generic routing encapsulation (l2gre) tunnel interface, use the **platform xconnect l2gre tunnel** command in VLAN interface mode.

platform xconnect l2gre *interface-num*

Syntax Description	<i>interface-num</i>	Specifies the tunnel interface number; valid values are 0 to 2147483647.
---------------------------	----------------------	--

Command Modes	VLAN interface mode (config-if)
----------------------	---------------------------------

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

Examples

The following example shows the how to configure the l2gre tunnel to 6:

```
Router # platform xconnect l2gre tunnel 6
```

Related Commands	Command	Description
	show platform l2transport gre	Displays platform details for l2gre tunnels.

police

To configure traffic policing, use the **police** command in policy-map class configuration mode or policy-map class police configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

```
police bps [burst-normal] [burst-max] conform-action action exceed-action action
[violate-action action]
```

```
no police bps [burst-normal] [burst-max] conform-action action exceed-action action
[violate-action action]
```

Syntax Description

<i>bps</i>	Average rate, in bits per second. Valid values are 8000 to 200000000.
<i>burst-normal</i>	(Optional) Normal burst size in bytes. Valid values are 1000 to 51200000. Default normal burst size is 1500.
<i>burst-max</i>	(Optional) Maximum burst size, in bytes. Valid values are 1000 to 51200000. Default varies by platform.
conform-action	Specifies action to take on packets that conform to the rate limit.
exceed-action	Specifies action to take on packets that exceed the rate limit.
violate-action	(Optional) Specifies action to take on packets that violate the normal and maximum burst sizes.

action

Action to take on packets. Specify one of the following keywords:

- **drop**—Drops the packet.
- **set-clp-transmit** *value*—Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet with the ATM CLP bit set to 1.
- **set-cos-inner-transmit** *value*—Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module when using bridging features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.
- **set-cos-transmit** *value*—Sets the COS packet value and sends it.
- **set-discard-class-transmit**—Sets the discard class attribute of a packet and transmits the packet with the new discard class setting.
- **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.
- **set-dscp-tunnel-transmit** *value*—Sets the DSCP value (0 to 63) in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking and transmits the packet with the new value.
- **set-frde-transmit** *value*—Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet with the DE bit set to 1.
- **set-mpls-experimental-imposition-transmit** *value*—Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers and transmits the packet with the new MPLS EXP bit value.
- **set-mpls-experimental-topmost** *value*—Rewrites the experimental value.
- **set-mpls-experimental-topmost-transmit** *value*—Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces.
- **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value.
- **set-prec-tunnel-transmit** *value*—Sets the precedence value (0 to 7) in the tunnel header of an L2TPv3 or GRE tunneled packet for tunnel marking and transmits the packet with the new value.
- **set-qos-transmit** *value*—Sets the qos-group value and transmits the packet with the new qos-group value.
- **transmit**—Transmits the packet. The packet is not altered.

Command Default

Traffic policing is not configured.

Command Modes

Policy-map class configuration (config-pmap-c) when specifying a single action to be applied to a marked packet

Policy-map class police configuration (config-pmap-c-police) when specifying multiple actions to be applied to a marked packet

Command History

Release	Modification
12.0(5)XE	This police command was introduced.
12.1(1)E	This command was integrated in Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T. The violate-action keyword was added.
12.2(2)T	The following modifications were made to the command: <ul style="list-style-type: none"> • The set-clp-transmit keyword for the <i>action</i> argument was added. • The set-frde-transmit keyword for the <i>action</i> argument was added. <p>Note However, the set-frde-transmit keyword is not supported for AToM traffic in this release. Also, the set-frde-transmit keyword is supported only when Frame Relay is implemented on a physical interface without encapsulation.</p> <ul style="list-style-type: none"> • The set-mpls-experimental-transmit keyword for the <i>action</i> argument was added.
12.2(8)T	The command was modified for the Policer Enhancement—Multiple Actions feature. This command can now accommodate multiple actions for packets marked as conforming to, exceeding, or violating a specific rate.
12.2(13)T	In the <i>action</i> argument, the set-mpls-experimental-transmit keyword was renamed to set-mpls-experimental-imposition-transmit .
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and the set-dscp-tunnel-transmit and set-prec-tunnel-transmit keywords for the <i>action</i> argument were added. These keywords are intended for marking Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packets.
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.
12.4(15)T2	This command was modified to include support for marking Generic Routing Encapsulation (GRE) tunneled packets. <p>Note For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF).</p>
15.1(1)T	This command was modified to include support for policing on SVI interfaces for Cisco ISR 1800, 2800, and 3800 series routers.
12.2(50)SY	Support for the set-mpls-experimental-topmost <i>action</i> argument was added.

Usage Guidelines

Use the **police** command to mark a packet with different quality of service (QoS) values based on conformance to the service-level agreement.

Traffic policing will not be executed for traffic that passes through an interface.

In Cisco IOS release 12.2(50)SY, when you apply the **set-mpls-experimental-topmost** *action* in the egress direction the **set-mpls-experimental-imposition** *action* is blocked.

Specifying Multiple Actions

The **police** command allows you to specify multiple policing actions. When specifying multiple policing actions when configuring the **police** command, note the following points:

- You can specify a maximum of four actions at one time.
- You cannot specify contradictory actions such as **conform-action transmit** and **conform-action drop**.

Using the Police Command with the Traffic Policing Feature

The **police** command can be used with the Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are in Cisco IOS Release 12.1(5)T: a single-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the **violate-action** option is not specified, and a two-token bucket system is used when the **violate-action** option is specified.

The token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.0(5)XE is different from the token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.1(5)T. For information on the token bucket algorithm introduced in Release 12.0(5)XE, see the *Traffic Policing* document for Release 12.0(5)XE. This document is available on the New Features for 12.0(5)XE documentation index (under Modular QoS CLI-related feature modules) at www.cisco.com.

The following are explanations of how the token bucket algorithms introduced in Cisco IOS Release 12.1(5)T work.

Token Bucket Algorithm with One Token Bucket

The one-token bucket algorithm is used when the **violate-action** option is not specified in the **police** command CLI.

The conform bucket is initially set to the full size (the full size is the number of bytes specified as the normal burst size).

When a packet of a given size (for example, “B” bytes) arrives at specific time (time “T”), the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time is T, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The token arrival rate is calculated as follows:

$$(\text{time between packets (which is equal to } T - T1) * \text{policer rate})/8 \text{ bytes}$$
- If the number of bytes in conform bucket B is greater than or equal to the packet size, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.
- If the number of bytes in conform bucket B (minus the packet size to be limited) is fewer than 0, the exceed action is taken.

Token Bucket Algorithm with Two Token Buckets

The two-token bucket algorithm is used when the **violate-action** option is specified in the **police** command.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, “B” bytes) arrives at specific time (time “T”) the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at T, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

The token arrival rate is calculated as follows:

$(\text{time between packets (which is equal to } T-T1) * \text{policer rate})/8 \text{ bytes}$

- If the number of bytes in conform bucket B is greater than or equal to the packet size, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in conform bucket B is less than the packet size, the excess token bucket is checked for bytes by the packet. If the number of bytes in exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number of bytes in exceed bucket B is less than the packet size, the packet violates the rate and the violate action is taken. The action is complete for the packet.

Using the set-cos-inner-transmit Action for SIPs and SPAs on the Cisco 7600 Series Router

The **set-cos-inner-transmit** keyword action was introduced in Cisco IOS Release 12.2(33)SRA to support marking of the inner CoS value as a policing action when using MPB features on the Enhanced FlexWAN module and when using MPB features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.

This command is not supported on the Cisco 7600 SIP-600.

For more information about QoS and the forms of **police** commands supported by the SIPs on the Cisco 7600 series router, see the *Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*.

Examples

Token Bucket Algorithm with One Token Bucket: Example

The following example shows how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the traffic policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, traffic policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0:

```
Router(config)# class-map access-match
```

```

Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting

```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the token bucket $((0.25 * 8000)/8)$, leaving 800 bytes in the token bucket. If the next packet is 900 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

Token Bucket Algorithm with Two Token Buckets: Example

In this example, traffic policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0.

```

Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action
set-qos-transmit 1 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting

```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet, and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket $((0.25 * 8000)/8)$, leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size), is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket).

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets $((.40 * 8000)/8)$. Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 bytes overflow the conform token bucket (because only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet, and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket $((.20 * 8000)/8)$. Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

Conforming to the MPLS EXP Value: Example

The following example shows that if packets conform to the rate limit, the MPLS EXP field is set to 5. If packets exceed the rate limit, the MPLS EXP field is set to 3.

```
Router(config)# policy-map input-IP-dscp
Router(config-pmap)# class dscp24
Router(config-pmap-c)# police 8000 1500 1000 conform-action
set-mpls-experimental-imposition-transmit 5 exceed-action
set-mpls-experimental-imposition-transmit 3
Router(config-pmap-c)# violate-action drop
```

Setting the Inner CoS Value as an Action for SIPs and SPAs on the Cisco 7600 Series Router: Example

The following example shows configuration of a QoS class that filters all traffic for virtual LAN (VLAN) 100 into a class named “vlan-inner-100” and establishes a traffic shaping policy for the vlan-inner-100 class. The service policy limits traffic to an average rate of 500 kbps, with a normal burst of 1000 bytes and a maximum burst of 1500 bytes, and sets the inner CoS value to 3. Since setting of the inner CoS value is supported only with bridging features, the configuration also shows the service policy being applied as an output policy for an ATM SPA interface permanent virtual circuit (PVC) that bridges traffic into VLAN 100 using the **bridge-domain** command.

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap)# class vlan-inner-100
Router(config-pmap-c)# police 500000 1000 1500 conform-action set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if-atm-vc)# end
```

Related Commands

Command	Description
bridge-domain	Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM PVC or Frame Relay data-link connection identifier (DLCI).
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Specifies the name of the service policy to be attached to the interface.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

port-channel hash-distribution

To set the hash distribution algorithm method, use the **port-channel hash-distribution** command in global configuration mode. To return to the default settings, use the **no** or **default** form of this command.

```
port-channel hash-distribution { adaptive | fixed }
```

```
{ no | default } port-channel hash-distribution
```

Syntax Description		
adaptive		Specifies selective distribution of the bundle select register among the port-channel members.
fixed		Specifies fixed distribution of the bundle select register among the port-channel members.
default		Specifies the default setting.

Command Default In Cisco IOS Release 12.2(50)SY or later releases, the hash distribution algorithm method is set to adaptive. In earlier releases, the hash distribution algorithm method is set to fixed.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SXH	This command was introduced.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines The EtherChannel load distribution algorithm uses the bundle select register in the port ASIC to determine the port for each outgoing packet. When you use the **adaptive** algorithm, it does not require the bundle select register to be changed for existing member ports. When you use the **fixed** algorithm and you either add or delete a port from the EtherChannel, the switch updates the bundle select register for each port in the EtherChannel. This update causes a short outage on each port.



Note

When you change the algorithm, the change is applied at the next member link event. Example events include link down, up, addition, deletion, no shutdown, and shutdown. When you enter the command to change the algorithm, the command console issues a warning that the command does not take effect until the next member link event.

Examples The following example shows how to set the hash distribution algorithm method to adaptive:

```
Router(config)# port-channel hash-distribution adaptive
```

priority-queue cos-map

To map CoS values to the receive and transmit strict-priority queues in interface configuration command mode, use the **priority-queue cos-map** command. To return to the default mapping, use the **no** form of this command.

priority-queue cos-map *queue-id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]]]

no priority-queue cos-map

Syntax Description

<i>queue-id</i>	Queue number; the valid value is 1 .
<i>cos1</i>	CoS value; valid values are from 0 to 7.
<i>... cos8</i>	(Optional) CoS values; valid values are from 0 to 7.

Command Default

The default mapping is queue 1 is mapped to CoS 5 for the following receive and transmit strict-priority queues:

- 1p1q4t receive queues
- 1p1q0t receive queues
- 1p1q8t receive queues
- 1p2q2t transmit queues
- 1p3q8t transmit queues
- 1p7q8t transmit queues
- 1p3q1t transmit queues
- 1p2q1t transmit queues

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

When mapping CoS values to the strict-priority queues, note the following information:

- The queue number is always **1**.
- You can enter up to 8 CoS values to map to the queue.

Examples

This example shows how to map CoS value 7 to the strict-priority queues on Gigabit Ethernet port 1/1:

```
Router(config-if)# priority-queue cos-map 1 7  
Router(config-if)#
```

Related Commands

Command	Description
show queueing interfaces	Displays queueing information.

priority-queue queue-limit

To set the priority-queue size on an interface, use the **priority-queue queue-limit** command in interface configuration mode. To return to the default priority-queue size, use the **no** form of this command.

priority-queue queue-limit *percent*

no priority-queue queue-limit *percent*

Syntax Description

percent Priority-queue size in percent; valid values are from 1 to 100.

Command Default

When global quality of service (QoS) is enabled the priority-queue size is 15. When global QoS is disabled the priority-queue size is 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF2	Support for this command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queuing-only** command or the **auto qos default** command is configured.

This command is supported on the following modules:

- WS-X6501-10GE—1p2q1t¹
- WS-X6148A-GE—1p3q8t²
- WS-X6148-45—1p3q8t
- WS-X6148-FE-SFP—1p3q8t
- WS-X6748-SFP—1p3q8t
- WS-X6724-SFP—1p7q8t³
- WS-X6704-10GE—1p7q4t⁴
- WS-SUP32-10GB-3E—1p7q4t

1. 1p2q1t—One strict-priority queue, two standard queues with one WRED drop threshold and one non-configurable (100%) tail-drop threshold per queue.
2. 1p3q8t—One strict-priority queue, three standard queues with eight WRED drop thresholds per queue.
3. 1p7q8t—One strict-priority queue, seven standard queues with eight WRED drop thresholds per queue.
4. 1p7q4t—One strict-priority queue, seven standard queues with four WRED drop thresholds per queue.

- WS-SUP32-GB-3E—1p3q8t
- WS-X6708-10GE—1p7q4t

Examples

The following example shows how to set the priority-queue size on an interface:

```
priority-queue queue-limit 15
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

queue-buffers ratio

To set the buffer ratio for a queue, use the **queue-buffers ratio** command in QoS policy-map class configuration mode. To remove the queue buffer ratio, use the **no** form of the command.

queue-buffers ratio *number*

no queue-buffers ratio *number*

Syntax Description	<i>number</i>	Sets the size of the queue ratio; valid range is 0 to 100.
--------------------	---------------	--

Command Default	None
-----------------	------

Command Modes	QoS policy-map class configuration (config-pmap-c)
---------------	--

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

Examples

The following example shows how to configure the buffer ratio to 6:

```
Router(config-pmap-c)# queue-buffers ratio 6
```

rcv-queue bandwidth

To define the bandwidths for ingress (receive) WRR queues through scheduling weights in interface configuration command mode, use the **rcv-queue bandwidth** command. To return to the default settings, use the **no** form of this command.

```
rcv-queue bandwidth weight-1 ... weight-n
```

```
no rcv-queue bandwidth
```

Syntax Description

weight-1 ... weight-n WRR weights; valid values are from 0 to 255.

Command Default

The defaults are as follows:

- QoS enabled—4:255
- QoS disabled—255:1

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

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

This command is supported on 2q8t and 8q8t ports only.

You can configure up to seven queue weights.

Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# rcv-queue bandwidth 3 1  
Router(config-if)#
```

Related Commands

Command	Description
rcv-queue queue-limit	Sets the size ratio between the strict-priority and standard receive queues.
show queueing interface	Displays queueing information.

rcv-queue cos-map

To map the class of service (CoS) values to the standard receive-queue drop thresholds, use the **rcv-queue cos-map** command in interface configuration mode. To remove the mapping, use the **no** form of this command.

```
rcv-queue cos-map queue-id threshold-id cos-1 ... cos-n
```

```
no rcv-queue cos-map queue-id threshold-id
```

Syntax Description

<i>queue-id</i>	Queue ID; the valid value is 1.
<i>threshold-id</i>	Threshold ID; valid values are from 1 to 4.
<i>cos-1 ... cos-n</i>	CoS values; valid values are from 0 to 7.

Command Default

The defaults are listed in [Table 1](#).

Table 1 CoS-to-Standard Receive Queue Map Defaults

queue	threshold	cos-map	queue	threshold	cos-map
With QoS Disabled			With QoS Enabled		
1	1	0,1, 2,3,4,5,6,7	1	1	0,1
1	2		1	2	2,3
1	3		1	3	4
1	4		1	4	6,7
2	1	5	2	1	5

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

The *cos-n* value is defined by the module and port type. When you enter the *cos-n* value, note that the higher values indicate higher priorities.

Use this command on trusted ports only.

Examples

This example shows how to map the CoS values 0 and 1 to threshold 1 in the standard receive queue:

```
Router (config-if)# rcv-queue cos-map 1 1 0 1  
cos-map configured on: Gi1/1 Gi1/2
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue queue-limit

To set the size ratio between the strict-priority and standard receive queues, use the **rcv-queue queue-limit** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
rcv-queue queue-limit q-limit-1 q-limit-2
```

```
no rcv-queue queue-limit
```

Syntax Description		
	<i>q-limit-1</i>	Standard queue weight; valid values are from 1 and 100 percent.
	<i>q-limit-2</i>	Strict-priority queue weight; see the “Usage Guidelines” section for valid values.

Command Default	The defaults are as follows: <ul style="list-style-type: none"> • 80 percent is for low priority. • 20 percent is for strict priority.
-----------------	--

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced.
	12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

Valid strict-priority weight values are from 1 to 100 percent, except on 1p1q8t ingress LAN ports, where valid values for the strict-priority queue are from 3 to 100 percent.

The **rcv-queue queue-limit** command configures ports on a per-ASIC basis.

Estimate the mix of strict-priority-to-standard traffic on your network (for example, 80-percent standard traffic and 20-percent strict-priority traffic) and use the estimated percentages as queue weights.

Examples

This example shows how to set the receive-queue size ratio for Gigabit Ethernet interface 1/2:

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue random-detect

To specify the minimum and maximum threshold for the specified receive queues, use the **rcv-queue random-detect** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
rcv-queue random-detect {max-threshold | min-threshold} queue-id threshold-percent-1 ...
threshold-percent-n
```

```
no rcv-queue random-detect {max-threshold | min-threshold} queue-id
```

Syntax Description

max-threshold	Specifies the maximum threshold.
min-threshold	Specifies the minimum threshold.
<i>queue-id</i>	Queue ID; the valid value is 1.
<i>threshold-percent-1</i> <i>threshold-percent-n</i>	Threshold weights; valid values are from 1 to 100 percent.

Command Default

The defaults are as follows:

- **min-threshold**—80 percent
- **max-threshold**—20 percent

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

This command is supported on 1p1q8t and 8q8t ports only.

The 1p1q8t interface indicates one strict queue and one standard queue with eight thresholds. The 8q8t interface indicates eight standard queues with eight thresholds. The threshold in the strict-priority queue is not configurable.

Each threshold has a low- and a high-threshold value. The threshold values are a percentage of the receive-queue capacity.

For additional information on configuring receive-queue thresholds, refer to the QoS chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to configure the low-priority receive-queue thresholds:

```
Router (config-if)# rcv-queue random-detect max-threshold 1 60 100
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.

rcv-queue threshold

To configure the drop-threshold percentages for the standard receive queues on 1p1q4t and 1p1q0t interfaces, use the **rcv-queue threshold** command in interface configuration mode. To return the thresholds to the default settings, use the **no** form of this command.

```
rcv-queue threshold queue-id threshold-percent-1 ... threshold-percent-n
```

```
no rcv-queue threshold
```

Syntax Description

<i>queue-id</i>	Queue ID; the valid value is 1.
<i>threshold-percent-1</i> ... <i>threshold-percent-n</i>	Threshold ID; valid values are from 1 to 100 percent.

Command Default

The defaults for the 1p1q4t and 1p1q0t configurations are as follows:

- Quality of service (QoS) assigns all traffic with class of service (CoS) 5 to the strict-priority queue.
- QoS assigns all other traffic to the standard queue.

The default for the 1q4t configuration is that QoS assigns all traffic to the standard queue.

If you enable QoS, the following default thresholds apply:

- 1p1q4t interfaces have this default drop-threshold configuration:
 - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue.
 - Using standard receive-queue drop threshold 1, the Cisco 7600 series router drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
 - Using standard receive-queue drop threshold 2, the Cisco 7600 series router drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
 - Using standard receive-queue drop threshold 3, the Cisco 7600 series router drops incoming frames with CoS 4 when the receive-queue buffer is 80 percent or more full.
 - Using standard receive-queue drop threshold 4, the Cisco 7600 series router drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.
 - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Cisco 7600 series router drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- 1p1q0t interfaces have this default drop-threshold configuration:
 - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue. The Cisco 7600 series router drops incoming frames when the receive-queue buffer is 100 percent full.
 - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Cisco 7600 series router drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.



Note

The 100-percent threshold may be actually changed by the module to 98 percent to allow Bridge Protocol Data Unite (BPDU) traffic to proceed. The BPDU threshold is factory set at 100 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines**Note**

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

The *queue-id* value is always 1.

A value of 10 indicates a threshold when the buffer is 10 percent full.

Always set threshold 4 to 100 percent.

Receive thresholds take effect only on ports whose trust state is trust cos.

Configure the 1q4t receive-queue tail-drop threshold percentages with the **wrr-queue threshold** command.

Examples

This example shows how to configure the receive-queue drop thresholds for Gigabit Ethernet interface 1/1:

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue threshold	Configures the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces.

show fips

To display the FIPs information about the switch, use the **show fips** command in EXEC mode.

show fips

no show fips

Syntax Description This command has no keywords or arguments

Syntax Description EXEC

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

Examples This example shows how to displays if FIPS modes if running on a switch:

```
Router# show fips
Router# The FIPS mode is on.
Router#
```

Related Commands	Command	Description
	fips	Enables FIPS security requirements on the switch.

show interfaces

To display statistics for all interfaces configured on the router or access server, use the **show interfaces** command in privileged EXEC mode.

Cisco 2500 Series, Cisco 2600 Series, Cisco 4700 Series, and Cisco 7000 Series

```
show interfaces [type number] [first] [last] [accounting]
```

Catalyst 6500 Series, Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor

```
show interfaces [type slot/port] [accounting | counters protocol status | crb | dampening |
description | dot1ad | etherchannel [module number] | fair-queue | irb | mac-accounting |
mpls-exp | precedence | random-detect | rate-limit | stats | summary | switching | utilization
{type number}]
```

Cisco 7500 Series with Ports on VIPs

```
show interfaces [type slot/port-adapter/port]
```

Cisco 7600 Series

```
show interfaces [type number | null interface-number | vlan vlan-id]
```

Channelized T3 Shared Port Adapters

```
show interfaces serial [slot/subslot/port/t1-num:channel-group]
```

Shared Port Adapters

```
show interfaces type [slot/subslot/port[/sub-int]]
```

Syntax Description

<i>type</i>	(Optional) Interface type. Allowed values for <i>type</i> can be atm , async , auto-template , bvi , bri0 , ctunnel , container , dialer , e1 , esconPhy , ethernet , fastethernet , fcpa , fdi , filter , filtergroup , gigabitethernet , ge-wan , hssi , longreachethernet , loopback , mfr , module , multilink , null , pos , port-channel , port-group , pos-channel , sbc , sdcc , serial , sysclock , t1 , tengigabitethernet , token , tokenring , tunnel , vif , vmi , virtual-access , virtual-ppp , virtual-template , virtual-tokenring , voaBypassIn , voaBypassOut , voaFilterIn , voaFilterOut , voaIn , voaOut .
Note	The type of interfaces available is based on the type of router used.
<i>number</i>	(Optional) Port number on the selected interface.

<i>first last</i>	(Optional) For Cisco 2500 series routers, ISDN Basic Rate Interface (BRI) only. The <i>first</i> argument can be either 1 or 2. The <i>last</i> argument can only be 2, indicating B channels 1 and 2. D-channel information is obtained by using the command without the optional arguments.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
counters protocol status	(Optional) Displays the current status of the protocol counters enabled.
crb	(Optional) Displays interface routing or bridging information.
dampening	(Optional) Displays interface dampening information.
description	(Optional) Displays the interface description.
dot1ad	(Optional) Displays interface 802.1ad information.
etherchannel [module number]	(Optional) Displays interface Ether Channel information. <ul style="list-style-type: none"> • module—The module keyword limits the display to interfaces available on the module.
fair-queue	(Optional) Displays interface Weighted Fair Queuing (WFQ) information.
irb	(Optional) Displays interface routing or bridging information.
mac-accounting	(Optional) Displays interface MAC accounting information.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays interface precedence accounting information.
random-detect	(Optional) Displays interface Weighted Random Early Detection (WRED) information.
rate-limit	(Optional) Displays interface rate-limit information.
stats	(Optional) Displays interface packets and octets, in and out, by using switching path.
summary	(Optional) Displays an interface summary.
switching	(Optional) Displays interface switching.
null interface-number	(Optional) Specifies the null interface, that is 0 .
<i>slot</i>	(Optional) Slot number. Refer to the appropriate hardware manual for slot information.
<i>/port</i>	(Optional) Port number. Refer to the appropriate hardware manual for port information.
<i>/port-adapter</i>	(Optional) Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.

[*slot/subslot/port/t1-num:channel-group*]

(Optional) Channelized T3 Shared Port Adapters

Number of the chassis slot that contains the channelized T3 Shared Port Adapters (SPA) (for example, 5/0/0:23), where:

- *slot*—(Optional) Chassis slot number.
For SPA interface processors (SIPs), refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
 - */subslot*—(Optional) Secondary slot number on a SIP where a SPA is installed.
Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
 - */port*—(Optional) Port or interface number.
For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide.
 - */t1-num*—(Optional) T1 time slot in the T3 line. The value can be from 1 to 28.
 - *:channel-group*—(Optional) Number 0–23 of the DS0 link on the T1 channel.
-

<i>[slot/subslot/port[/sub-int]]</i>	(Optional) Shared Port Adapters
	<p>Number of the chassis slot that contains the SPA interface (for example, 4/3/0), where:</p> <ul style="list-style-type: none"> • <i>slot</i>—(Optional) Chassis slot number. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide. • <i>/subslot</i>—(Optional) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information. • <i>/port</i>—(Optional) Port or interface number. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide. • <i>/sub-int</i>—(Optional) Subinterface number (for those SPAs that support subinterface configuration).
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	This command was modified to include support for flow-based WRED.
12.0(4)T	This command was modified to include enhanced display information for dialer bound interfaces.
12.0(7)T	This command was modified to include dialer as an interface type and to reflect the default behavior.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S2	This command was integrated into Cisco IOS Release 12.2(20)S2 and introduced a new address format and output for SPA interfaces on the Cisco 7304 router. The <i>subslot</i> argument was introduced.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.2(14)SX	This command was modified. Support for this command was introduced.
12.2(17d)SXB	This command was modified. The uplink dual-mode port information was updated.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers, and the tengigabitethernet interface type was added. 10-Gigabit Ethernet interfaces were introduced with the release of the 1-Port 10-Gigabit Ethernet SPA.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SXJ01	This command was integrated into Cisco IOS Release 12.2(33)SXJ01.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB1	This command was updated to display operational status for Gigabit Ethernet interfaces that are configured as primary and backup interfaces (Cisco 7600 series routers).
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command was modified. The default value of the command was modified on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(50)SY	This command was integrated in Cisco IOS Release 12.2(50)SY and the dot1ad keyword was added.
15.0(01)SY	This command was integrated in Cisco IOS Release 15.1(50)SY.

Usage Guidelines

Display Interpretation

The **show interfaces** command displays statistics for the network interfaces. The resulting output varies, depending on the network for which an interface has been configured. The resulting display on the Cisco 7200 series routers shows the interface processors in slot order. If you add interface processors after booting the system, they will appear at the end of the list, in the order in which they were inserted.

Information About Specific Interfaces

The *number* argument designates the module and port number. If you use the **show interfaces** command on the Cisco 7200 series routers without the *slot/port* arguments, information for all interface types will be shown. For example, if you type **show interfaces** you will receive information for all Ethernet, serial, Token Ring, and FDDI interfaces. Only by adding the type *slot/port* argument you can specify a particular interface.

Cisco 7600 Series Routers

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

The port channels from 257 to 282 are internally allocated and are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

Statistics are collected on a per-VLAN basis for Layer 2-switched packets and Layer 3-switched packets. Statistics are available for both unicast and multicast traffic. The Layer 3-switched packet counts are available for both ingress and egress directions. The per-VLAN statistics are updated every 5 seconds.

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config** commands. In this case, the duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command shows the operating mode for an interface, and the **show running-config** command shows the configured mode for an interface.

If you do not enter any keywords, all counters for all modules are displayed.

Command Variations

You will use the **show interfaces** command frequently while configuring and monitoring devices. The various forms of the **show interfaces** commands are described in detail in the sections that follow.

Dialer Interfaces Configured for Binding

If you use the **show interfaces** command on dialer interfaces configured for binding, the display will report statistics on each physical interface bound to the dialer interface; see the following examples for more information.

Removed Interfaces

If you enter a **show interfaces** command for an interface type that has been removed from the router or access server, interface statistics will be displayed accompanied by the following text: “Hardware has been removed.”

Weighted Fair Queueing Information

If you use the **show interfaces** command on a router or access server for which interfaces are configured to use weighted fair queueing through the **fair-queue** interface command, additional information is displayed. This information consists of the current and high-water mark number of flows.

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, when a multilink PPP (MLP) interface is down/down, its default bandwidth rate is the sum of the serial interface bandwidths associated with the MLP interface.

In Cisco IOS Release 12.2(31)SB, the default bandwidth rate is 64 Kbps.

Examples



Note

The following is sample output from the **show interfaces** command. Because your display will depend on the type and number of interface cards in your router or access server, only a portion of the display is shown.

If an asterisk (*) appears after the throttles counter value, it means that the interface was throttled at the time the command was run.

```
Router# show interfaces

Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 10.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
```

```

ARP type: ARPA, ARP Timeout 4:00:00
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters 0:00:00
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 4 packets/sec
  1127576 packets input, 447251251 bytes, 0 no buffer
    Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  5332142 packets output, 496316039 bytes, 0 underruns
    0 output errors, 432 collisions, 0 interface resets, 0 restarts
.
.
.

```

Example with Custom Output Queueing

The following shows partial sample output when custom output queueing is enabled:

```

Router# show interfaces

Last clearing of "show interface" counters 0:00:06
Input queue: 0/75/0 (size/max/drops); Total output drops: 21
Output queues: (queue #: size/max/drops)
  0: 14/20/14  1: 0/20/6  2: 0/20/0  3: 0/20/0  4: 0/20/0  5: 0/20/0
  6: 0/20/0  7: 0/20/0  8: 0/20/0  9: 0/20/0  10: 0/20/0
.
.
.

```

When custom queueing is enabled, the drops accounted for in the output queues result from bandwidth limitation for the associated traffic and lead to queue length overflow. Total output drops include drops on all custom queues and the system queue. Fields are described with the weighted fair queueing output in [Table 2](#).

Example Including Weighted-Fair-Queueing Output

For each interface on the router or access server configured to use weighted fair queueing, the **show interfaces** command displays the information beginning with *Input queue:* in the following display:

```

Router# show interfaces

Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 10.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 4 packets/sec
    1127576 packets input, 447251251 bytes, 0 no buffer
      Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5332142 packets output, 496316039 bytes, 0 underruns
      0 output errors, 432 collisions, 0 interface resets, 0 restarts
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Output queue: 7/64/0 (size/threshold/drops)
    Conversations 2/9 (active/max active)

```


Table 2 describes the input queue and output queue fields shown in the preceding two displays.

Table 2 *Weighted-Fair-Queueing Output Field Descriptions*

Field	Description
Input Queue	
size	Current size of the input queue.
max	Maximum size of the queue.
drops	Number of messages discarded in this interval.
Total output drops	Total number of messages discarded in this session.
Output Queue	
size	Current size of the output queue.
threshold	Congestive-discard threshold. Number of messages in the queue after which new messages for high-bandwidth conversations are dropped.
drops	Number of dropped messages.
Conversations: active	Number of currently active conversations.
Conversations: max active	Maximum number of concurrent conversations allowed.

Example with Accounting Option

To display the number of packets of each protocol type that have been sent through all configured interfaces, use the **show interfaces accounting** command. When you use the **accounting** option, only the accounting statistics are displayed.



Note

Except for protocols that are encapsulated inside other protocols, such as IP over X.25, the accounting option also shows the total bytes sent and received, including the MAC header. For example, it totals the size of the Ethernet packet or the size of a packet that includes High-Level Data Link Control (HDLC) encapsulation.

Per-packet accounting information is kept for the following protocols:

- AppleTalk
- Address Resolution Protocol (ARP) (for IP, Frame Relay, Switched Multimegabit Data Service (SMDS))
- Connectionless Network Service (CLNS)
- Digital Equipment Corporation (DEC) Maintenance Operations Protocol (MOP)

The routers use MOP packets to advertise their existence to Digital Equipment Corporation machines that use the MOP. A router periodically broadcasts MOP packets to identify itself as a MOP host. This results in MOP packets being counted, even when DECnet is not being actively used.

- DECnet
- HP Probe
- IP
- LAN Manager (LAN Network Manager and IBM Network Manager)

- Novell
- Serial Tunnel Synchronous Data Link Control (SDLC)
- Spanning Tree
- SR Bridge
- Transparent Bridge

Example with DWRED

The following is sample output from the **show interfaces** command when distributed WRED (DWRED) is enabled on an interface. Notice that the packet drop strategy is listed as “VIP-based weighted RED.”

```
Router# show interfaces hssi 0/0/0

Hssi0/0/0 is up, line protocol is up
  Hardware is cyBus HSSI
  Description: 45Mbps to R1
  Internet address is 10.200.14.250/30
  MTU 4470 bytes, BW 45045 Kbit, DLY 200 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:02, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Packet Drop strategy: VIP-based weighted RED
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  1976 packets input, 131263 bytes, 0 no buffer
  Received 1577 broadcasts, 0 runts, 0 giants
  0 parity
  4 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  1939 packets output, 130910 bytes, 0 underruns
  0 output errors, 0 applique, 3 interface resets
  0 output buffers copied, 0 interrupts, 0 failures
```

Example with ALC

The following is sample output from the **show interfaces** command for serial interface 2 when Airline Control (ALC) Protocol is enabled:

```
Router# show interfaces serial 2

Serial2 is up, line protocol is up
  Hardware is CD2430
  MTU 1500 bytes, BW 115 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation ALC, loopback not set
  Full-duplex enabled.
    ascus in UP state: 42, 46
    ascus in DOWN state:
    ascus DISABLED:
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 3 interface resets
  0 output buffer failures, 0 output buffers swapped out
```

DCD=down DSR=down DTR=down RTS=down CTS=down

Example with SDLC

The following is sample output from the **show interfaces** command for an SDLC primary interface supporting the SDLC function:

```
Router# show interfaces

Serial 0 is up, line protocol is up
Hardware is MCI Serial
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation SDLC-PRIMARY, loopback not set
  Timers (msec): poll pause 100 fair poll 500. Poll limit 1
  [T1 3000, N1 12016, N2 20, K 7] timer: 56608 Last polled device: none
  SDLLC [ma: 0000.0C01.14--, ring: 7 bridge: 1, target ring: 10
    largest token ring frame 2052]
SDLC addr C1 state is CONNECT
  VS 6, VR 3, RCNT 0, Remote VR 6, Current retransmit count 0
  Hold queue: 0/12 IFRAMES 77/22 RNRs 0/0 SNRMs 1/0 DISCs 0/0
  Poll: clear, Poll count: 0, chain: p: C1 n: C1
  SDLLC [largest SDLC frame: 265, XID: disabled]
Last input 00:00:02, output 00:00:01, output hang never
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 517 bits/sec, 30 packets/sec
Five minute output rate 672 bits/sec, 20 packets/sec
  357 packets input, 28382 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  926 packets output, 77274 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets, 0 restarts
  2 carrier transitions
```

[Table 3](#) shows the fields relevant to all SDLC connections.

Table 3 *show interfaces Field Descriptions When SDLC Is Enabled*

Field	Description
Timers (msec)	List of timers in milliseconds.
poll pause, fair poll, Poll limit	Current values of these timers.
T1, N1, N2, K	Current values for these variables.

Table 4 shows other data given for each SDLC secondary interface configured to be attached to this interface.

Table 4 SDLC Field Descriptions

Field	Description
addr	Address of this secondary interface.
State	Current state of this connection. The possible values follow: <ul style="list-style-type: none"> • BOTHBUSY—Both sides have told each other that they are temporarily unable to receive any more information frames. • CONNECT—A normal connect state exists between this router and this secondary. • DISCONNECT—No communication is being attempted to this secondary. • DISCSENT—This router has sent a disconnect request to this secondary and is awaiting its response. • ERROR—This router has detected an error, and is waiting for a response from the secondary acknowledging this. • SNRMSENT—This router has sent a connect request (SNRM) to this secondary and is awaiting its response. • THEMBUSY—This secondary has told this router that it is temporarily unable to receive any more information frames. • USBUSY—This router has told this secondary that it is temporarily unable to receive any more information frames.
VS	Sequence number of the next information frame this station sends.
VR	Sequence number of the next information frame from this secondary that this station expects to receive.
RCNT	Number of correctly sequenced I-frames received when the Cisco IOS software was in a state in which it is acceptable to receive I-frames.
Remote VR	Last frame transmitted by this station that has been acknowledged by the other station.
Current retransmit count	Number of times the current I-frame or sequence of I-frames has been retransmitted.
Hold queue	Number of frames in hold queue/Maximum size of hold queue.
IFRAMEs, RNRs, SNRMs, DISCs	Sent and received count for these frames.
Poll	“Set” if this router has a poll outstanding to the secondary; “clear” if it does not.
Poll count	Number of polls, in a row, given to this secondary at this time.
chain	Shows the previous (p) and next (n) secondary address on this interface in the round-robin loop of polled devices.

Sample show interfaces accounting Display

The following is sample output from the **show interfaces accounting** command:

```
Router# show interfaces accounting
```

```

Interface TokenRing0 is disabled

Ethernet0
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
          IP      873171   735923409   34624     9644258
          Novell  163849   12361626    57143     4272468
          DEC MOP    0         0           1          77
          ARP      69618    4177080    1529      91740
Interface Serial0 is disabled

Ethernet1
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
          IP        0         0           37        11845
          Novell    0         0           4591     275460
          DEC MOP    0         0           1          77
          ARP        0         0           7         420

Interface Serial11 is disabled
Interface Ethernet2 is disabled
Interface Serial2 is disabled
Interface Ethernet3 is disabled
Interface Serial3 is disabled
Interface Ethernet4 is disabled
Interface Ethernet5 is disabled
Interface Ethernet6 is disabled
Interface Ethernet7 is disabled
Interface Ethernet8 is disabled
Interface Ethernet9 is disabled

Fddi0
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
          Novell    0         0           183      11163
          ARP        1         49           0         0

```

When the output indicates that an interface is “disabled,” the router has received excessive errors (over 5000 in a keepalive period).

Example with Flow-Based WRED

The following is sample output from the **show interfaces** command issued for the serial interface 1 for which flow-based WRED is enabled. The output shows that there are 8 active flow-based WRED flows, that the maximum number of flows active at any time is 9, and that the maximum number of possible flows configured for the interface is 16:

```

Router# show interfaces serial 1

Serial11 is up, line protocol is up

  Hardware is HD64570
  Internet address is 10.1.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  Reliability 255/255, txload 237/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive not set
  Last input 00:00:22, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:17:58
  Input queue: 0/75/0 (size/max/drops); Total output drops: 2479
  Queuing strategy: random early detection(WRED)
    flows (active/max active/max): 8/9/16
    mean queue depth: 27
  drops: class  random  tail    min-th  max-th  mark-prob
          0      946    0      20     40     1/10

```

```

1      488      0      22      40      1/10
2      429      0      24      40      1/10
3      341      0      26      40      1/10
4      235      0      28      40      1/10
5       40      0      31      40      1/10
6       0       0      33      40      1/10
7       0       0      35      40      1/10
  rsvp  0       0      37      40      1/10
30 second input rate 1000 bits/sec, 2 packets/sec
30 second output rate 119000 bits/sec, 126 packets/sec
  1346 packets input, 83808 bytes, 0 no buffer
  Received 12 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  84543 packets output, 9977642 bytes, 0 underruns
  0 output errors, 0 collisions, 6 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up

```

Example with DWFO

The following is sample output from the **show interfaces** command when distributed weighted fair queueing (DWFO) is enabled on an interface. Notice that the queueing strategy is listed as “VIP-based fair queueing.”

```

Router# show interfaces fastethernet 1/1/0

Fast Ethernet 1/1/0 is up, line protocol is up
  Hardware is cyBus Fast Ethernet Interface, address is 0007.f618.4448 (bia 00e0)
  Description: pkt input i/f for WRL tests (to pagent)
  Internet address is 10.0.2.70/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, fdx, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 01:11:01, output hang never
  Last clearing of "show interface" counters 01:12:31
  Queueing strategy: VIP-based fair queueing
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 0 multicast
    0 input packets with dribble condition detected
    1 packets output, 60 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffers copied, 0 interrupts, 0 failures

```

Example with DNIS Binding

When the **show interfaces** command is issued on an unbound dialer interface, the output looks as follows:

```

Router# show interfaces dialer0

Dialer0 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.1.1.2/8
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 3/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset

```

```

Last input 00:00:34, output never, output hang never
Last clearing of "show interface" counters 00:05:09
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 1000 bits/sec, 0 packets/sec
  18 packets input, 2579 bytes
  14 packets output, 5328 bytes

```

But when the **show interfaces** command is issued on a bound dialer interface, you will get an additional report that indicates the binding relationship. The output is shown here:

```

Router# show interfaces dialer0

Dialer0 is up, line protocol is up
  Hardware is Unknown
  Internet address is 10.1.1.2/8
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Interface is bound to BRI0:1
  Last input 00:00:38, output never, output hang never
  Last clearing of "show interface" counters 00:05:36

Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    38 packets input, 4659 bytes
    34 packets output, 9952 bytes

Bound to:
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  Interface is bound to Dialer0 (Encapsulation PPP)
  LCP Open, multilink Open
  Last input 00:00:39, output 00:00:11, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    78 packets input, 9317 bytes, 0 no buffer
  Received 65 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  93 packets output, 9864 bytes, 0 underruns
  0 output errors, 0 collisions, 7 interface resets
  0 output buffer failures, 0 output buffers swapped out
  4 carrier transitions

```

At the end of the Dialer0 output, the **show interfaces** command is executed on each physical interface bound to it.

Example with BRI

In this example, the physical interface is the B1 channel of the BRI0 link. This example also illustrates that the output under the B channel keeps all hardware counts that are not displayed under any logical or virtual access interface. The line in the report that states "Interface is bound to Dialer0 (Encapsulation

LAPB)" indicates that this B interface is bound to Dialer0 and the encapsulation running over this connection is Link Access Procedure, Balanced (LAPB), not PPP, which is the encapsulation configured on the D interface and inherited by the B channel.

```
Router# show interfaces bri0:1
```

```
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  Interface is bound to Dialer0 (Encapsulation LAPB)
  LCP Open, multilink Open
  Last input 00:00:31, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
    110 packets input, 13994 bytes, 0 no buffer
    Received 91 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    135 packets output, 14175 bytes, 0 underruns
    0 output errors, 0 collisions, 12 interface resets
    0 output buffer failures, 0 output buffers swapped out
    8 carrier transitions
```

Any protocol configuration and states should be displayed from the Dialer0 interface.

Example with a Fast Ethernet SPA on a Cisco 7304 Router

The following is sample output from the **show interfaces fastethernet** command for the second interface (port 1) in a 4-Port 10/100 Fast Ethernet SPA located in the bottom subslot (1) of the Modular Service Cards (MSC) that is installed in slot 2 on a Cisco 7304 router:

```
Router# show interfaces fastethernet 2/1/1
```

```
FastEthernet2/1/1 is up, line protocol is up
  Hardware is SPA-4FE-7304, address is 00b0.64ff.5d80 (bia 00b0.64ff.5d80)
  Internet address is 192.168.50.1/24
  MTU 9216 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:22, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    5 packets input, 320 bytes
    Received 1 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
    8 packets output, 529 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    2 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```


Example for an Interface with an Asymmetric Receiver and Transmitter Rates

```
Router# show interfaces e4/0
```

```
Ethernet4/0 is up, line protocol is up
  Hardware is AmdP2, address is 000b.bf30.f470 (bia 000b.bf30.f470)
  Internet address is 10.1.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, RxBW 5000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 254/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:03:36
  Input queue: 34/75/0/819 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 7138000 bits/sec, 14870 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  3109298 packets input, 186557880 bytes, 0 no buffer
  Received 217 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 input packets with dribble condition detected
  22 packets output, 1320 bytes, 0 underruns
  11 output errors, 26 collisions, 0 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
```

Table 5 describes the significant fields shown in the display.

Table 5 *show interfaces fastethernet Field Descriptions—Fast Ethernet SPA*

Field	Description
Fast Ethernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, SPA-4FE-7304) and MAC address.
Description	Alphanumeric string identifying the interface. This appears only if the description interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 4-Port 10/100 Fast Ethernet SPA.
BW	Bandwidth of the interface in kilobits per second.
RxBW	Receiver bandwidth of the interface, in kilobits per second. This value is displayed only when an interface has asymmetric receiver and transmitter rates.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.

Table 5 *show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)*

Field	Description
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
100Mb/s, 10Mb/s	Speed of the interface in megabits per second.
100BaseTX/FX	Media protocol standard.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed. Note This field does not apply to SPA interfaces.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: <ul style="list-style-type: none"> • Size—Number of packets in the input queue. • Max—Maximum size of the queue. • Drops—Number of packets dropped because of a full input queue. • Flushes—Number of packets dropped as part of selective packet discard (SPD). SPD implements a selective packet drop policy on the router’s IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.

Table 5 *show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)*

Field	Description
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is first-in, first-out (FIFO).
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. Note For the 4-Port 10/100 Fast Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the maximum transmission unit (MTU) for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, cyclic redundancy check (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.

Table 5 *show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)*

Field	Description
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired. Expiration happens when receiving a packet with a length greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.

Table 5 *show interfaces fastethernet Field Descriptions—Fast Ethernet SPA (continued)*

Field	Description
no carrier	Number of times the carrier was not present during the transmission. Note This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 4-Port 10/100 Fast Ethernet SPA on the Cisco 7304 router.

Example with a Gigabit Ethernet SPA on a Cisco 7304 Router

The following is sample output from the **show interfaces gigabitethernet** command for the first interface (port 0) in a 2-Port 10/100/1000 Gigabit Ethernet SPA located in the top subslot (0) of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show interfaces gigabitethernet 4/0/0

GigabitEthernet4/0/0 is up, line protocol is down
  Hardware is SPA-2GE-7304, address is 00b0.64ff.5a80 (bia 00b0.64ff.5a80)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 1000Mb/s, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    109 packets output, 6540 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    1 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

Example with Gigabit Ethernet SPAs Configured as Primary and Backup Interfaces on a Cisco 7600 Router

The following examples show the additional lines included in the display when the command is issued on two Gigabit Ethernet interfaces that are configured as a primary interface (gi3/0/0) and as a backup interface (gi3/0/11) for the primary:

```
Router# show interfaces gigabitEthernet 3/0/0

GigabitEthernet3/0/0 is up, line protocol is up (connected)
  Hardware is GigEther SPA, address is 0005.dc57.8800 (bia 0005.dc57.8800)
  Backup interface GigabitEthernet3/0/11, failure delay 0 sec, secondary disable delay 0 sec,
  .
  .
  .

Router# show interfaces gigabitEthernet 3/0/11

GigabitEthernet3/0/11 is standby mode, line protocol is down (disabled)
```

·
·
·

Table 6 describes the fields shown in the display for Gigabit Ethernet SPA interfaces.

Table 6 *show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA*

Field	Description
GigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, SPA-2GE-7304) and MAC address.
Backup interface	Identifies the backup interface that exists for this, the primary interface.
Failure and secondary delay	The period of time (in seconds) to delay bringing up the backup interface when the primary goes down, and bringing down the backup after the primary becomes active again. On the Cisco 7600 router, the delay must be 0 (the default) to ensure that there is no delay between when the primary goes down and the backup comes up, and vice versa.
Standby mode	Indicates that this is a backup interface and that it is currently operating in standby mode.
Description	Alphanumeric string identifying the interface. This appears only if the description interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 2-Port 10/100/1000 Gigabit Ethernet SPA.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
1000Mb/s, 100Mb/s, 10Mb/s	Speed of the interface in megabits per second.
link type	Specifies whether autonegotiation is being used on the link.
media type	Interface port media type: RJ45, SX, LX, or ZX.
100BaseTX/FX	Media protocol standard.
ARP type:	Type of ARP assigned and the timeout period.

Table 6 show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA (continued)

Field	Description
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed. Note This field does not apply to SPA interfaces.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: <ul style="list-style-type: none"> • Size—Number of packets in the input queue. • Max—Maximum size of the queue. • Drops—Number of packets dropped because of a full input queue. • Flushes—Number of packets dropped as part of SPD. SPD implements a selective packet drop policy on the router’s IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Table 6 *show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA (continued)*

Field	Description
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. Note For the 2-Port 10/100/1000 Gigabit Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the MTU for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired. Expiration happens when receiving a packet with a length greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.

Table 6 *show interfaces gigabitethernet Field Descriptions—Gigabit Ethernet SPA (continued)*

Field	Description
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission. Note This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 2-Port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.

Example with a Packet over SONET/SDH (POS) SPA on a Cisco 7600 Series Router and Catalyst 6500 Series Switch

The following is sample output from the **show interfaces pos** command on a Cisco 7600 series router or Catalyst 6500 series switch for POS interface 4/3/0 (which is the interface for port 0 of the SPA in subslot 3 of the SIP in chassis slot 4):

```
Router# show interfaces pos 4/3/0

POS4/3/0 is up, line protocol is up (APS working - active)
  Hardware is Packet over SONET
  Internet address is 10.0.0.1/8
  MTU 4470 bytes, BW 622000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Scramble disabled
  Last input 00:00:34, output 04:09:06, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    Available Bandwidth 622000 kilobits/sec
```

```

5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  782 packets input, 226563 bytes, 0 no buffer
  Received 0 broadcasts, 1 runts, 0 giants, 0 throttles
    0 parity
  1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  271 packets output, 28140 bytes, 0 underruns
  0 output errors, 0 applique, 2 interface resets
  0 output buffer failures, 0 output buffers swapped out
  2 carrier transitions
    
```

Table 7 describes the significant fields shown in this display.

Table 7 *show interfaces pos Field Descriptions—POS SPA*

Field	Description
POS4/3/0 is up, line protocol is up	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.
Hardware is. . .	Hardware type: <ul style="list-style-type: none"> • For POSIP—cyBus Packet over SONET • For POS SPAs—Packet over SONET
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the bandwidth interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Indicates whether loopbacks are set.
Keepalive	Indicates whether keepalives are set.
Scramble	Indicates whether SONET payload scrambling is enabled. SONET scrambling is disabled by default. For the POS SPAs on the Cisco 12000 series routers, scrambling is enabled by default.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.

Table 7 *show interfaces pos Field Descriptions—POS SPA (continued)*

Field	Description
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with number of packets ignored. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.

Table 7 *show interfaces pos Field Descriptions—POS SPA (continued)*

Field	Description
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
applique	Indicates an unrecoverable error has occurred on the POSIP applique. The system then invokes an interface reset.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Example with a POS SPA on a Cisco 12000 Series Router

The following is sample output from the **show interfaces pos** command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces pos 1/1/0

POS1/1/0 is up, line protocol is up
  Hardware is Packet over SONET
  Internet address is 10.41.41.2/24
  MTU 4470 bytes, BW 9952000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive not set
  Scramble enabled
  Last input 00:00:59, output 00:00:11, output hang never
  Last clearing of "show interface" counters 00:00:14
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    Available Bandwidth 9582482 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1 packets output, 314 bytes, 0 underruns
    0 output errors, 0 applique, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```

Example with a POS SPA SDCC Interface on a Cisco 12000 Series Router

The following is sample output from the **show interfaces sdcc** command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces sdcc 1/1/0

SDCC1/1/0 is administratively down, line protocol is down
  Hardware is SDCC
  MTU 1500 bytes, BW 192 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:01:55
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```

Table 8 describes the significant fields shown in the display.

Table 8 *show interfaces sdcc Field Descriptions—POS SPA*

Field	Description
SDCC1/1/0 is administratively down, line protocol is down	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.
Hardware is. . .	Hardware type is SDCC—Section Data Communications Channel.
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the bandwidth interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
crc	Cyclic redundancy check size (16 or 32 bits).
Loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Table 8 *show interfaces sdcc Field Descriptions—POS SPA (continued)*

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2 ³¹ ms (and less than 2 ³² ms) ago.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with number of packets ignored. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.

Table 8 *show interfaces sdcc Field Descriptions—POS SPA (continued)*

Field	Description
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Not supported for POS interfaces.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Example with a T3/E3 Shared Port Adapter

The following example shows the interface serial statistics on the first port of a T3/E3 SPA installed in subslot 0 of the SIP located in chassis slot 5:

```
Router# show interfaces serial 5/0/0

Serial5/0/0 is up, line protocol is up
  Hardware is SPA-4T3E3
  Internet address is 10.1.1.2/24
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
```



```

reliability 255/255, txload 234/255, rxload 234/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Last input 00:00:05, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 40685000 bits/sec, 115624 packets/sec
5 minute output rate 40685000 bits/sec, 115627 packets/sec
 4653081241 packets input, 204735493724 bytes, 0 no buffer
  Received 4044 broadcasts (0 IP multicast)
   0 runts, 0 giants, 0 throttles
    0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 4652915555 packets output, 204728203520 bytes, 0 underruns
  0 output errors, 0 applique, 4 interface resets
  0 output buffer failures, 0 output buffers swapped out
 2 carrier transitions

```

Table 9 describes the fields shown in the **show interfaces serial** output for a T3/E3 SPA.



Note The fields appearing in the output will vary depending on card type, interface configuration, and the status of the interface.

Table 9 *show interfaces serial Field Descriptions—T3/E3 SPA*

Field	Description
Serial	Name of the serial interface.
line protocol is	If the line protocol is up, the local router has received keepalive packets from the remote router. If the line protocol is down, the local router has not received keepalive packets from the remote router.
Hardware is	Designates the specific hardware type of the interface.
Internet address is	The IP address of the interface.
MTU	The maximum packet size set for the interface.
BW	Bandwidth in kilobits per second.
DLY	Interface delay in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method.
crc	CRC size in bits.
loopback	Indicates whether loopback is set.

Table 9 *show interfaces serial Field Descriptions—T3/E3 SPA (continued)*

Field	Description
keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing of show interface counters	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 milliseconds (and less than 232 ms) ago.
Input queue	Packet statistics on the input queue reported as: <ul style="list-style-type: none"> • Size—Current size of the input queue. • Max—Maximum size of the input queue. • Drops—Packets dropped because the queue was full. • Flushes—Number of times that data on queue has been discarded.
Total output drops	Total number of dropped packets.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in the output queue (size), and the maximum size of the queue (max).

Table 9 *show interfaces serial Field Descriptions—T3/E3 SPA (continued)*

Field	Description
5-minute input rate	<p>Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic).</p> <p>The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.</p>
5-minute output rate	<p>Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic).</p> <p>The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.</p>

Example with a 1-Port 10-Gigabit Ethernet SPA on a Cisco 12000 Series Router

The following is sample output from the **show interfaces tengigabitethernet** command for the only interface (port 0) in a 1-Port 10 Gigabit Ethernet SPA located in the top subslot (0) of the carrier card that is installed in slot 7 on a Cisco 12000 series router:

```
Router# show interfaces tengigabitethernet 7/0/0

TenGigabitEthernet7/0/0 is up, line protocol is up (connected)
  Hardware is TenGigEther SPA, address is 0000.0c00.0102 (bia 000f.342f.c340)
  Internet address is 10.1.1.2/24
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:10, output hang never
  Last clearing of "show interface" counters 20:24:30
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
    237450882 packets input, 15340005588 bytes, 0 no buffer
    Received 25 broadcasts (0 IP multicasts)
```

```

0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
1676 packets output, 198290 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out

```

Table 10 describes the significant fields shown in the display.

Table 10 *show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA*

Field	Description
TenGigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type and MAC address.
Description	Alphanumeric string identifying the interface. This appears only if the description interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
10Gb/s	Speed of the interface in Gigabits per second.
input flow control ...	Specifies if input flow control is on or off.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.

Table 10 *show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA*

Field	Description
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed.
Last clearing	<p>Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared.</p> <p>A series of asterisks (***) indicates the elapsed time is too large to be displayed.</p> <p>0:00:00 indicates the counters were cleared more than 2^{31} ms (and less than 2^{32} ms) ago.</p>
Input queue (size/max/drops/flushes)	<p>Packet statistics on the input queue reported as:</p> <ul style="list-style-type: none"> • Size—Number of packets in the input queue. • Max—Maximum size of the queue. • Drops—Number of packets dropped because of a full input queue. • Flushes—Number of packets dropped as part of SPD. SPD implements a selective packet drop policy on the router’s IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	<p>Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic).</p> <p>The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.</p>

Table 10 *show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA*

Field	Description
L2 Switched	Provides statistics about Layer 2 switched traffic, including unicast and multicast traffic.
L3 in Switched	Provides statistics about received Layer 3 traffic.
L3 out Switched	Provides statistics about sent Layer 3 traffic.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired.
multicast	Number of multicast packets.
pause input	Number of pause packets received.

Table 10 *show interfaces tengigabitethernet Field Descriptions—10-Gigabit Ethernet SPA*

Field	Description
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
pause output	Number of pause packets transmitted.
output buffer failures, output buffers swapped out	Number of output buffers failures and output buffers swapped out.

Displaying Traffic for a Specific Interface Example

This example shows how to display traffic for a specific interface:

```
Router# show interfaces GigabitEthernet1/1
```

```
GigabitEthernet0/1 is up, line protocol is up
  Hardware is BCM1125 Internal MAC, address is 0016.9de5.d9d1 (bia 0016.9de5.d9d1)
  Internet address is 172.16.165.40/27
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
```

```

Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is XON, input flow-control is XON
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:11, output 00:00:08, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 10 packets input, 2537 bytes, 0 no buffer
  Received 10 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 46 multicast, 0 pause input
  0 input packets with dribble condition detected
 18 packets output, 3412 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  7 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  2 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out
    
```



Note

The unknown protocol drops field displayed in the above example refers to the total number of packets dropped due to unknown or unsupported types of protocol. This field occurs on several platforms such as the Cisco 3725, 3745, 3825, and 7507 series routers.

This example shows how to display traffic for a FlexWAN module:

```

Router# show interfaces pos 6/1/0.1

POS6/1/0.1 is up, line protocol is up
  Hardware is Packet over Sonet
  Internet address is 10.1.2.2/24
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY <<<+++ no packets info after this line
Arches#sh mod 6
Mod Ports Card Type                               Model                               Serial No.
-----
  6    0  2 port adapter FlexWAN                    WS-X6182-2PA                       SAD04340JY3

Mod MAC addresses                                Hw   Fw           Sw           Status
-----
  6   0001.6412.a234 to 0001.6412.a273  1.3  12.2(2004022 12.2(2004022 Ok

Mod Online Diag Status
-----
  6 Pass
Router#
    
```

Related Commands

Command	Description
fair-queue	Enables WFQ.
interface	Configures an interface type and enters interface configuration mode.

Command	Description
show controllers fastethernet	Displays Fast Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers pos	Displays information about the POS controllers.
show controllers serial	Displays controller statistics.

show ip cef platform

To display entries in the Forwarding Information Base (FIB) or to display a summary of the FIB, use the **show ip cef platform** command in privileged EXEC mode.

```
show ip cef ip-prefix [mask] platform [checksum | detail | internal checksum]
```

Syntax Description

<i>ip-prefix</i> [mask]	The IP address prefix of the entries to display. You can also include an optional subnet mask.
checksum	(Optional) Displays FIB entry checksums information.
detail	(Optional) Displays detailed FIB entry information.
internal { checksum }	(Optional) Displays internal data structures. The checksum option includes FIB entry checksums information in the output.

Command Default

None

Command History

Privileged EXEC (#)

Command History

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

Examples

The following example shows FIB entry information for IP address prefix 10.4.4.4:

```
Router# show ip cef 10.4.4.4 platform

10.4.4.4/32
Fib Entry: 0xD6680610 XCM leaf from 0x50805550(RP) 0xA0805550(FP):
load_bal_or_adj[0] 0x0 load_bal_or_adj[1] 0x18 load_bal_or_adj[2] 0x1C
leaf points to an adjacency, index 0x607
ip_mask 0x0 as_number 0x0 precedence_num_loadbal_intf 0xF0 qos_group 0x0
Label object OCE Chain:
Label(0x12, real) Adjacency
c10k_label_data = 0x450467F8
tag_elt_addr = 0x50003038
ipv6_tag_elt_addr = 0x0
tag_index = 0x607
tt_tag_rew = 0x45046800
Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
mac_rewrite_index = 0x395, flags = 0x9
pktswitched = 0 byteswitched = 0
XCM Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
mac_rewrite_index = 0x395, flags = 0x9
mac_index_extension = 0x0
XCM mac rewrite from index 0x395
mtu from 0x53800E54(RP) 0xA3800E54(FP)
frag_flags = 0x0
mtu = 1496
mac length 0x12 encap length 0x16 upd_offset=0x02FF
```

```
mac string start from bank4 0x32001CA8(RP)
0x82001CA8(FP)
mac string end from bank9 0x50801CA8(RP)
0xA0801CA8(FP)
Encap String: 0005DC387B180003A011A57881000002884700012000
```

Related Commands

Command	Description
show cef	Displays which packets the line cards dropped, or displays which packets were not express forwarded.
show cef interface	Displays Cisco Express Forwarding-related interface information.

show ipv6 cef platform

To display platform-specific Cisco Express Forwarding (CEF) data, use the **show ipv6 cef platform** command in user EXEC or privileged EXEC mode.

show ipv6 cef platform [checksum | detail | internal]

Syntax Description	checksum	(Optional) Displays FIB entry checksums.
	detail	(Optional) Displays detailed platform-specific Cisco Express Forwarding data.
	internal	(Optional) Displays internal platform-specific Cisco Express Forwarding data.

Command Default None

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines If none of the optional keywords are used, data for all of the platforms is displayed.

Examples The following example displays all platform-specific Cisco Express Forwarding data:

```
Router# show ipv6 cef platform
```

show mac address-table

To display the MAC address table, use the **show mac address-table** command in privileged EXEC mode.

```
show mac address-table [address mac-addr [all | interface type/number | module number | vlan vlan-id] | [count [module number | vlan vlan-id]] | [interface type/number] | [limit [vlan vlan-id | module number | interface interface-type]] | [module number] | [multicast [count | igmp-snooping | mld-snooping [count] | user [count] | vlan vlan-id]]] | [notification {mac-move [counter [vlan] | threshold | change] | interface [interface-number]]] | [synchronize statistics] | [unicast-flood] | vlan vlan-id [module number]]
```

Syntax	Description
address <i>mac-addr</i>	(Optional) Displays information about the MAC address table for a specific MAC address. See the “Usage Guidelines” section for formatting information.
all	(Optional) Displays every instance of the specified MAC address in the forwarding table.
interface <i>type/number</i>	(Optional) Displays addresses for a specific interface; valid values are atm , fastethernet , gigabitethernet , and port-channel .
module <i>number</i>	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
vlan <i>vlan-id</i>	(Optional) Displays addresses for a specific VLAN, valid values are from 1 to 4094.
count	(Optional) Displays the number of entries that are currently in the MAC address table.
limit	Displays MAC-usage information.
multicast	Displays information about the multicast MAC address table entries only.
igmp-snooping	Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
mld-snooping	Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
user	Displays the manually entered (static) addresses.
notification mac-move	Displays the MAC-move notification status.
notification mac-move counter	(Optional) Displays the number of times a MAC has moved and the number of these instances that have occurred in the system.
notification threshold	Displays the Counter-Addressable Memory (CAM) table utilization notification status.
notification change	Displays the MAC notification parameters and history table.
synchronize statistics	Displays information about the statistics collected on the switch processor or DFC.
unicast-flood	Displays unicast-flood information.

Command Modes Privileged EXEC (#)

Command History

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

Usage Guidelines

If you do not specify a module number, the output of the **show mac address-table** command displays information about the supervisor engine. To display information about the MAC address table of the DFCs, you must enter the module number or the **all** keyword.

The *mac-addr* value is a 48-bit MAC address. The valid format is H.H.H.

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

The optional **module number** keyword and argument are supported only on DFC modules. The **module number** keyword and argument designate the module number.

Valid values for the *mac-group-address* argument are from 1 to 9.

The optional **count** keyword displays the number of multicast entries.

The optional **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The information that is displayed in the **show mac address-table unicast-flood** command output is as follows:

- Up to 50 flood entries, shared across all the VLANs that are not configured to use the filter mode, can be recorded.
- The output field displays are defined as follows:
 - ALERT—Information is updated approximately every 3 seconds.
 - SHUTDOWN—Information is updated approximately every 3 seconds.



Note The information displayed on the destination MAC addresses is deleted as soon as the floods stop after the port shuts down.

- Information is updated each time that you install the filter. The information lasts until you remove the filter.

The dynamic entries that are displayed in the Learn field are always set to Yes.

The **show mac address-table limit** command output displays the following information:

- The current number of MAC addresses.
- The maximum number of MAC entries that are allowed.
- The percentage of usage.

The **show mac address-table synchronize statistics** command output displays the following information:

- Number of messages processed at each time interval.
- Number of active entries sent for synchronization.
- Number of entries updated, created, ignored, or failed.

Examples

The following is sample output from the **show mac address-table** command:

```
Switch# show mac address-table

Dynamic Addresses Count:          9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:     41
Total MAC addresses:             50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-----
0010.0de0.e289      Dynamic      1     FastEthernet0/1
0010.7b00.1540      Dynamic      2     FastEthernet0/5
0010.7b00.1545      Dynamic      2     FastEthernet0/5
0060.5cf4.0076      Dynamic      1     FastEthernet0/1
0060.5cf4.0077      Dynamic      1     FastEthernet0/1
0060.5cf4.1315      Dynamic      1     FastEthernet0/1
0060.70cb.f301      Dynamic      1     FastEthernet0/1
00e0.1e42.9978      Dynamic      1     FastEthernet0/1
00e0.1e9f.3900      Dynamic      1     FastEthernet0/1
```

**Note**

In a distributed Encoded Address Recognition Logic (EARL) switch, the asterisk (*) indicates a MAC address that is learned on a port that is associated with this EARL.

This example shows how to display the information about the MAC address table for a specific MAC address with a Supervisor Engine 720:

```
Router# show mac address-table address 001.6441.60ca
```

Codes: * - primary entry

```
      vlan  mac address  type  learn qos  ports
-----+-----+-----+-----+-----
Supervisor:
* --- 0001.6441.60ca  static No  -- Router
```

This example shows how to display MAC address table information for a specific MAC address with a Supervisor Engine 720:

```
Router# show mac address-table address 0100.5e00.0128
```

Legend: * - primary entry
age - seconds since last seen
n/a - not available

```
      vlan  mac address  type  learn  age  ports
-----+-----+-----+-----+-----+-----
Supervisor:
* 44 0100.5e00.0128  static Yes  - Fa6/44, Router
* 1 0100.5e00.0128  static Yes  - Router
Module 9:
* 44 0100.5e00.0128  static Yes  - Fa6/44, Router
* 1 0100.5e00.0128  static Yes  - Router
```

This example shows how to display the currently configured aging time for all VLANs:

```
Router# show mac address-table aging-time
```

```
Vlan    Aging Time
----    -
*100    300
200     1000
```

This example shows how to display the entry count for a specific slot:

```
Router# show mac address-table count module 1
```

```
MAC Entries on slot 1 :
Dynamic Address Count:          4
Static Address (User-defined) Count: 25
Total MAC Addresses In Use:     29
Total MAC Addresses Available:  131072
```

This example shows how to display the information about the MAC address table for a specific interface with a Supervisor Engine 720:

```
Router# show mac address-table interface fastethernet 6/45
```

```
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available
```

vlan	mac address	type	learn	age	ports
* 45	00e0.f74c.842d	dynamic	Yes	5	Fa6/45



Note

A leading asterisk (*) indicates entries from a MAC address that was learned from a packet coming from an outside device to a specific module.

This example shows how to display the limit information for a specific slot:

```
Router# show mac address-table limit vlan 1 module 1
```

vlan	switch	module	action	maximum	Total entries	flooding
1	1	7	warning	500	0	enabled
1	1	11	warning	500	0	enabled
1	1	12	warning	500	0	enabled

```
Router# show mac address-table limit vlan 1 module 2
```

vlan	switch	module	action	maximum	Total entries	flooding
1	2	7	warning	500	0	enabled
1	2	9	warning	500	0	enabled

The following example shows how to display the MAC-move notification status:

```
Router# show mac address-table notification mac-move
```

```
MAC Move Notification: Enabled
Router#
```

The following example shows how to display the MAC move statistics:

```
Router> show mac address-table notification mac-move counter
```



```
-----
Vlan Mac Address From Mod/Port To Mod/Port Count
-----
```

```
1 00-01-02-03-04-01 2/3 3/1 10
20 00-01-05-03-02-01 5/3 5/1 20
```

This example shows how to display the CAM-table utilization-notification status:

```
Router# show mac address-table notification threshold
```

```
Status limit Interval
```

```
-----+-----+-----
enabled 1 120
```

This example shows how to display the MAC notification parameters and history table:

```
Router# show mac address-table notification change
```

```
MAC Notification Feature is Disabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
```

```
-----
Interface                MAC Added Trap MAC Removed Trap
-----
```

This example shows how to display the MAC notification parameters and history table for a specific interface:

```
Router# show mac address-table notification change interface gigabitethernet5/2
```

```
MAC Notification Feature is Disabled on the switch
```

```
Interface                MAC Added Trap MAC Removed Trap
```

```
-----
GigabitEthernet5/2      Disabled        Disabled
```

This example shows how to display unicast-flood information:

```
Router# show mac address-table unicast-flood
```

```
> > Unicast Flood Protection status: enabled
```

```
> >
```

```
> > Configuration:
```

```
> > vlan Kfps action timeout
```

```
> > -----+-----+-----+-----+-----
```

```
> > 2 2 alert none
```

```
> >
```

```
> > Mac filters:
```

```
> > No. vlan source mac addr. installed
```

```
> > on time left (mm:ss)
```

```
> >
```

```
> > -----+-----+-----+-----+-----
```

```
> >
```

```
> > Flood details:
```

```
> > Vlan source mac addr. destination mac addr.
```

```
> >
```

```
> > -----+-----+-----+-----+-----
```

```
> > 2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
```

```
> > 0000.0000.bac0
```

```
> > 0000.0000.bac2, 0000.0000.bac4,
```

```
> > 0000.0000.bac6
```

```
> > 0000.0000.bac8
```

```
> > 2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
> > 0000.0000.bac1
> > 0000.0000.bac3, 0000.0000.bac5,
> > 0000.0000.bac7
> > 0000.0000.bac9
```

This example shows how to display the information about the MAC address table for a specific VLAN:

```
Router# show mac address-table vlan 1300
```

```
      vlan mac address      type   learn  age           ports
-----+-----+-----+-----+-----+-----
*    1300 2000.0000.0031  dynamic Yes      0           VPLS peer 100.0.0.77(2:1)
```

This example shows how to display the information about the MAC address table for MLDv2 snooping:

```
Router# show mac address-table multicast mld-snooping
```

```
vlan mac address type learn qos ports
-----+-----+-----+-----+-----+-----
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch
```

Related Commands

Command	Description
clear mac address-table	Deletes entries from the MAC address table.
mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mac address-table limit	Enables MAC limiting.
mac address-table notification mac-move	Enables MAC-move notification.
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.
mac address-table synchronize	Synchronizes the Layer 2 MAC address table entries across the PFC and all the DFCs.
show mac address-table static	Displays static MAC address table entries only.

show mac address-table aging-time

To display the MAC address aging time, use the **show mac address-table aging-time** command in privileged EXEC mode.

```
show mac address-table aging-time [vlan vlan-id]
```

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1005.
---------------------------	--

Command Modes	Privileged EXEC (#)
----------------------	---------------------

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

Examples The following example shows how to display the current configured aging time for all VLANs. The fields shown in the display are self-explanatory.

```
Router# show mac address-table aging-time
```

```
Vlan      Aging Time
----      -
100       300
200       1000
```

The following example shows how to display the current configured aging time for a specific VLAN. The fields shown in the display are self-explanatory.

```
Router# show mac address-table aging-time vlan 100
```

```
Vlan      Aging Time
----      -
100       300
```

Related Commands	Command	Description
	show mac address-table address	Displays MAC address table information for a specific MAC address.
	show mac address-table count	Displays the number of entries currently in the MAC address table.
	show mac address-table detail	Displays detailed MAC address table information.
	show mac address-table dynamic	Displays dynamic MAC address table entries only.
	show mac address-table interface	Displays the MAC address table information for a specific interface.
	show mac address-table multicast	Displays multicast MAC address table information.
	show mac address-table protocol	Displays MAC address table information based on protocol.

Command	Description
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for a specific VLAN.

show mac address-table dynamic

To display dynamic MAC address table entries only, use the **show mac address-table dynamic** command in privileged EXEC mode.

```
show mac address-table dynamic [{address mac-addr} | {interface interface interface-num [all | module number]}] | {module num} | {vlan vlan-id [all | module number]}
```

Syntax Description		
address <i>mac-addr</i>	(Optional) Specifies a 48-bit MAC address; valid format is H.H.H.	
interface <i>interface interface-num</i>	(Optional) Specifies an interface to match. Valid type values are FastEthernet and GigabitEthernet, valid number values are from 1 to 9.	
all	(Optional) Specifies that the output display all dynamic MAC address table entries.	
module <i>num</i>	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.	
vlan <i>vlan-</i>	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 1005.	

Command Modes Privileged EXEC (#)

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

Usage Guidelines The *mac-address* is a 48-bit MAC address and the valid format is H.H.H.

The optional **module num** keyword and argument are supported only on DFC modules. The **module num** keyword and argument designate the module number.

Examples This example shows how to display all the dynamic MAC address entries for a specific VLAN.

```
Router# show mac address-table dynamic vlan 200 all
```

```
Legend: * - primary entry
         age - seconds since last seen
         n/a - not available
vlan    mac address      type   learn   age      ports
-----+-----+-----+-----+-----+-----
 200 0010.0d40.37ff  dynamic NO      23      Gi5/8
Router#
```

This example shows how to display all the dynamic MAC address entries.

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

```
Legend: * - primary entry
         age - seconds since last seen
         n/a - not applicable
vlan    mac address      type   learn   age      ports
```

```

-----+-----+-----+-----+-----+-----
* 10  0010.0000.0000  dynamic  Yes  n/a      Gi4/1
* 3   0010.0000.0000  dynamic  Yes   0       Gi4/2
* 1   0002.fcbc.ac64  dynamic  Yes  265     Gi8/1
* 1   0009.12e9.adc0  static   No    -       Router
Router#
    
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for a specific MAC address.
show mac address-table aging-time	Displays the MAC address aging time.
show mac address-table count	Displays the number of entries currently in the MAC address table.
show mac address-table detail	Displays detailed MAC address table information.
show mac address-table interface	Displays the MAC address table information for a specific interface.
show mac address-table multicast	Displays multicast MAC address table information.
show mac address-table protocol	Displays MAC address table information based on protocol.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for a specific VLAN.

show mac address-table learning

To display the MAC address learning state, use the **show mac address-table learning** command in user EXEC mode.

```
show mac address-table learning [vlan vlan-id | interface interface slot/port] [module num]
```

Syntax Description

vlan <i>vlan-id</i>	(Optional) Displays information about the MAC address learning state for the specified switch port VLAN; valid values are from 1 to 4094.
interface <i>interface slot/port</i>	(Optional) Displays information about the MAC address learning state for the specified routed interface type, the slot number, and the port number.
module <i>num</i>	(Optional) Displays information about the MAC address learning state for the specified module number.

Defaults

This command has no default settings.

Command Modes

User EXEC (>)

Command History

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

Usage Guidelines

The **module** *num* keyword and argument can be used to specify supervisor engines or Distributed Forwarding Cards (DFCs) only.

The **interface** *interface slot/port* keyword and arguments can be used on routed interfaces only. The **interface** *interface slot/port* keyword and arguments cannot be used to configure learning on switch port interfaces.

If you specify the **vlan** *vlan-id*, the state of the MAC address learning of the specified VLAN on all modules, including router interfaces, is displayed.

If you specify the **vlan** *vlan-id* and the **module** *num*, the state of the MAC address learning of a specified VLAN on a specified module is displayed.

If you specify the **interface** *interface slot/port* keyword and arguments, the state of the MAC address learning of the specified interface on all modules is displayed.

If you specify the **interface** *interface slot/port* keyword and arguments, the state of the MAC address learning of the specified interface on the specified module is displayed.

If you enter the **show mac address-table learning** command with no arguments or keywords, the status of MAC learning on all the existing VLANs on all the supervisor engines or DFCs configured on a Cisco 7600 series router is displayed.

Examples

This example shows how to display the MAC address learning status on all the existing VLANs on all of the supervisor engines or DFCs configured on a Cisco 7600 series router:

```
Router# show mac address-table learning

VLAN/Interface      Mod1   Mod4   Mod7
-----
1                   yes    yes    yes
100                 yes    yes    yes
150                 yes    yes    yes
200                 yes    yes    yes
250                 yes    yes    yes
1006                no     no     no
1007                no     no     no
1008                no     no     no
1009                no     no     no
1010                no     no     no
1011                no     no     no
1012                no     no     no
1013                no     no     no
1014                no     no     no
GigabitEthernet6/1 no     no     no
GigabitEthernet6/2 no     no     no
GigabitEthernet6/4 no     no     no
FastEthernet3/4    no     no     no
FastEthernet3/5    no     no     no
GigabitEthernet4/1 no     no     no
GigabitEthernet4/2 no     no     no
GigabitEthernet7/1 no     no     no
GigabitEthernet7/2 no     no     no
```

Router#

Table 11 describes the fields that are shown in the example.

Table 11 show mac address-table learning Field Descriptions

Field	Description
VLAN/Interface ¹	VLAN ID or interface type, module, and port number.
Mod#	Module number of a supervisor engine or DFC.
yes	MAC address learning is enabled.
no	MAC address learning is disabled.

1. The interfaces displayed are routed interfaces that have internal VLANs assigned to them.

This example shows how to display the status of MAC address learning on all the existing VLANs on a single supervisor engine or a DFC:

```
Router# show mac address-table learning module 4

VLAN/Interface      Mod4
-----
1                   yes
100                 yes
150                 yes
200                 yes
250                 yes
1006                no
1007                no
1008                no
```



```

1009                no
1010                no
1011                no
1012                no
1013                no
1014                no
GigabitEthernet6/1 no
GigabitEthernet6/2 no
GigabitEthernet6/4 no
FastEthernet3/4    no
FastEthernet3/5    no
GigabitEthernet4/1 no
GigabitEthernet4/2 no
GigabitEthernet7/1 no
GigabitEthernet7/2 no

```

Router#

This example shows how to display the status of MAC address learning for a specific VLAN on all the supervisor engines and DFCs:

Router# **show mac address-table learning vlan 100**

```

VLAN   Mod1   Mod4   Mod7
-----
100    no     no     yes

```

Router

This example shows how to display the status of MAC address learning for a specific VLAN on a specific supervisor engine or DFC:

Router# **show mac address-table learning vlan 100 module 7**

```

VLAN   Mod7
-----
100    yes

```

Router

This example shows how to display the status of MAC address learning for a specific supervisor engine or DFC:

Router# **show mac address-table learning interface FastEthernet 3/4**

```

Interface   Mod1   Mod4   Mod7
-----
Fa3/4       no     yes    no

```

Router

This example shows how to display the status of MAC address learning for a specific interface on a specific supervisor engine or DFC:

Router# **show mac address-table learning interface FastEthernet 3/4 module 1**

```

Interface   Mod1
-----
Fa3/4       no

```

Router

Related Commands

Command	Description
mac address-table learning	Enables MAC address learning.

show mac address-table static

To display static MAC address table entries only, use the **show mac address-table static** command in privileged EXEC mode.

```
show mac address-table static [address mac-address | aging-time routed-mac | interface type
                               number | module number | notification {change | mac-move} | synchronize statistics | vlan
                               vlan-id]
```

Syntax Description

address mac-address	(Optional) Specifies a 48-bit MAC address to match; valid format is H.H.H.
aging-type routed-mac	(Optional) Specifies the routed MAC address status.
detail	(Optional) Specifies a detailed display of MAC address table information.
interface type number	(Optional) Specifies an interface to match; valid type values are Ethernet, FastEthernet, and Gigabit Ethernet and valid number values are from 1 to 9.
module number	(Optional) Specifies a module to match; valid values are from 1 to 4.
notification change	(Optional) Specifies the MAC address notification parameters and history table.
notification mac-move	(Optional) Specifies status for the MAC address move notifications.
synchronize statistics	(Optional) Specifies the statistics for MAC address synchronization.
vlan vlan	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 1005.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The keyword definitions for the protocol argument are:

- **ip**—Specifies IP protocol.
- **ipx**—Specifies Internetwork Packet Exchange (IPX) protocols.
- **assigned**—Specifies assigned protocol entries.
- **other**—Specifies other protocol entries.

Examples

The following examples show how to display the static MAC address entries:

```
Router# show mac address-table static

*Oct 22 12:15:35: %SYS-5-CONFIG_I: Configured from console by console
vlan  mac address      type  protocol  qos      ports
-----+-----+-----+-----+-----+-----
 200  0050.3e8d.6400  static  assigned  --  Router
 100  0050.3e8d.6400  static  assigned  --  Router
```

```

4092 0050.f0ac.3058 static other -- Router
917 0100.0cdd.dddd static other -- Fa5/9,Router,Switch
5 0050.3e8d.6400 static assigned -- Router
303 0100.0cdd.dddd static other -- Fa5/9,Router,Switch
850 0100.0cdd.dddd static other -- Fa5/9,Router,Switch
1002 0100.0cdd.dddd static other -- Fa5/9,Router,Switch
802 0100.0cdd.dddd static other -- Fa5/9,Router,Switch
2 0100.0cdd.dddd static other -- Fa5/9,Router,Switch
304 0100.5e00.0001 static ip -- Fa5/9,Switch
.

```

The following example shows how to display static MAC address entries with a specific protocol type (in this case, assigned):

```
Router# show mac address-table static protocol assigned
```

```

vlan mac address type protocol qos ports
-----+-----+-----+-----+-----+-----
200 0050.3e8d.6400 static assigned -- Router
100 0050.3e8d.6400 static assigned -- Router
5 0050.3e8d.6400 static assigned -- Router

```

The following example shows the detailed output for the previous example:

```
Router# show mac address-table static protocol assigned detail
```

```

MAC Table shown in details
=====
Type Always Learn Trap Modified Notify Capture Protocol Flood
-----+-----+-----+-----+-----+-----+-----+-----+
QoS bit L3 Spare Mac Address Age Byte Pvlan Xtag SWbits Index
-----+-----+-----+-----+-----+-----+-----+-----+
STATIC NO NO NO NO NO assigned NO
Bit Not On 0 0050.3e8d.6400 254 200 1 0 0x3
STATIC NO NO NO NO NO assigned NO
Bit Not On 0 0050.3e8d.6400 254 100 1 0 0x3
STATIC NO NO NO NO NO assigned NO
Bit Not On 0 0050.3e8d.6400 254 5 1 0 0x3
S Bit Not On 0 0050.f0ac.3058 254 4092 1 0 0x3
.

```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for a specific MAC address.
show mac address-table aging-time	Displays the MAC address aging time.
show mac address-table count	Displays the number of entries currently in the MAC address table.
show mac address-table detail	Displays detailed MAC address table information.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for a specific interface.
show mac address-table multicast	Displays multicast MAC address table information.

Command	Description
show mac address-table protocol	Displays MAC address table information based on protocol.
show mac address-table vlan	Displays the MAC address table information for a specific VLAN.

show mvr

To display the current Multicast VLAN Registration (MVR) global parameter values, including whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible), use the **show mvr** privileged EXEC command.

show mvr

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

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

Examples This is an example of output from the **show mvr** command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the preceding display, the maximum number of multicast groups is fixed at 256. The MVR mode is either compatible (for interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with IGMP snooping operation and dynamic MVR membership on source ports is supported).

Related Commands	Command	Description
	mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
	mvr (interface configuration)	Configures MVR ports.
	show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the interface and members keywords are appended to the command.
	show mvr members	Displays all ports that are members of an MVR multicast group or, if there are no members, means the group is inactive.

show mvr interface

To display the Multicast VLAN Registration (MVR) receiver and source ports, use the **show mvr interface** privileged EXEC command without keywords. Use the command with keywords to display MVR parameters for a specific receiver port.

```
show mvr interface [interface-id [members [vlan vlan-id]]]
```

Syntax Description

<i>interface-id</i>	(Optional) Displays MVR type, status, and Immediate Leave setting for the interface; valid interfaces include physical ports (including type, stack member [stacking-capable switches only] module, and port number).
members	(Optional) Displays all MVR groups to which the specified interface belongs.
vlan <i>vlan-id</i>	(Optional) Displays all MVR group members on this VLAN. The range is 1 to 4094.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

If the entered port identification is a non-MVR port or a source port, the command returns an error message. For receiver ports, it displays the port type, per port status, and Immediate-Leave setting.

If you enter the **members** keyword, all MVR group members on the interface appear. If you enter a VLAN ID, all MVR group members in the VLAN appear.

Examples

This is an example of output from the **show mvr interface** command:

```
Switch# show mvr interface
Port      Type      Status      Immediate Leave
----      -
Gi1/0/1   SOURCE    ACTIVE/UP   DISABLED
Gi1/0/2   RECEIVER  ACTIVE/DOWN DISABLED
```

In the preceding display, Status is defined as follows:

- Active means the port is part of a VLAN.
- Inactive means that the port is not yet part of any VLAN.
- Up/Down means that the port is forwarding/nonforwarding.

This is an example of output from the **show mvr interface** command for a specified port:

```
Switch# show mvr interface gigabitethernet1/0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This is an example of output from the **show mvr interface *interface-id* members** command:

```
Switch# show mvr interface gigabitethernet1/0/2 members
239.255.0.0      DYNAMIC ACTIVE
239.255.0.1      DYNAMIC ACTIVE
239.255.0.2      DYNAMIC ACTIVE
239.255.0.3      DYNAMIC ACTIVE
239.255.0.4      DYNAMIC ACTIVE
239.255.0.5      DYNAMIC ACTIVE
239.255.0.6      DYNAMIC ACTIVE
239.255.0.7      DYNAMIC ACTIVE
239.255.0.8      DYNAMIC ACTIVE
239.255.0.9      DYNAMIC ACTIVE
```

Related Commands	Command	Description
	mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
	mvr (interface configuration)	Configures MVR ports.
	show mvr	Displays the global MVR configuration on the switch.
	show mvr members	Displays all receiver ports that are members of an MVR multicast group.

show mvr members

To display all receiver and source ports that are currently members of an IP multicast group, use the **show mvr members** privileged EXEC command.

```
show mvr members [ip-address]
```

Syntax Description	<i>ip-address</i>	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as Inactive.
--------------------	-------------------	---

Command Modes	Privileged EXEC
---------------	-----------------

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

Usage Guidelines The **show mvr members** command applies to receiver and source ports. For MVR-compatible mode, all source ports are members of all multicast groups.

Examples This example shows the status of all mvr members:

```
Switch# show mvr members
MVR Group IP      Status      Members
-----
239.255.0.1      ACTIVE      Gi1/0/1(d), Gi1/0/5(s)
239.255.0.2      INACTIVE    None
239.255.0.3      INACTIVE    None
239.255.0.4      INACTIVE    None
239.255.0.5      INACTIVE    None
239.255.0.6      INACTIVE    None
239.255.0.7      INACTIVE    None
239.255.0.8      INACTIVE    None
239.255.0.9      INACTIVE    None
239.255.0.10     INACTIVE    None
```

<output truncated>

This example shows the status of an IP address and the members of the IP multicast group with that IP address:

```
Switch# show mvr members 239.255.0.2
239.255.003.--22  ACTIVE      Gi1//1(d), Gi1/0/2(d), Gi1/0/3(d),
                  Gi1/0/4(d), Gi1/0/5(s)
```


Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the members keyword is appended to the command.

show platform acl

To display ACL software-switched setting, use the **show platform acl** command.

```
show platform acl {software-switched}
```

Syntax	Description
software-switched	Displays the ACL software-switched setting.

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 display software-switched platform ACLs:

```
Router# show platform acl software-switched
```

Related Commands	Command	Description
	platform acl software-switched	Configures the platform ACL software-switched settings.

show platform acl software-switched

To display whether ACLs are enabled for software-switched WAN packets, use the **show platform acl software-switched** command in privileged EXEC mode.

show platform acl software-switched

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

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

Usage Guidelines By default, ACLs are not applied to packets that are software-switched between WAN cards and the route processor. To determine whether ACLs are enabled for software-switched ingress or egress WAN packets, use the **show platform acl software-switched** command.

Examples This example shows how to display whether ACLs are enabled for software-switched WAN packets:

```
Router# show platform acl software-switched
CWAN: ACL treatment for software switched in INGRESS is enabled
CWAN: ACL treatment for software switched in EGRESS is disabled
```

Related Commands	Command	Description
	platform cwan acl software-switched	Allows ACLs to be applied to WAN packets that are software-switched.

show platform bridge

To display distributed or hardware-based bridging information, use the **show platform bridge** command in privileged EXEC mode.

show platform bridge [*interface-type interface-number*] [**vlan** *vlan-id*] [**summary**]

Syntax Description	
<i>interface-type</i>	(Optional) Interface type and number.
<i>interface-number</i>	
vlan <i>vlan-id</i>	(Optional) Displays VLAN bridging information.
summary	(Optional) Displays a summary of bridging information.

Command Default None

Command Modes Privileged EXEC (#)

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

Examples The following is sample output from the **show platform bridge** command:

Router# **show platform bridge**

```

VLAN Interface          CircuitId  LTL   PseudoPort  State  Options
 12 PO1/1/3.1           102      0xC3F   1/256    up    dot1q
 13 PO1/1/3.1           103      0xC3F   1/256    up    dot1q
 14 PO1/1/3.2           104      0xC3F   1/256    up    default
 15 PO1/1/3.2           105      0xC3F   1/256    up    default
 16 PO1/1/3.3           106      0xC3F   1/256    up    dot1q-tunnel
 17 PO1/1/3.3           107      0xC3F   1/256    up    dot1q-tunnel
 41 Gi8/0/17            1201     0xDE2   8/227    up    access
 41 Gi8/0/17            1202     0xDE3   8/228    up    access
 41 Gi8/0/17            1203     0xDE4   8/229    up    access
 41 Gi8/0/17            1204     0xDE5   8/230    up    access
 41 Gi8/0/17            1205     0xDE6   8/231    up    access
 41 Gi8/0/17            1206     0xDE7   8/232    up    access
 41 Gi8/0/17            1207     0xDE8   8/233    up    access
 41 Gi8/0/17            1208     0xDE9   8/234    up    access
 41 Gi8/0/17            1209     0xDEA   8/235    up    access
 41 Gi8/0/17            1210     0xDEB   8/236    up    access
 41 Gi8/0/17            1211     0xDEC   8/237    up    access
 41 Gi8/0/17            1212     0xDED   8/238    up    access
 41 Gi8/0/17            1213     0xDEE   8/239    up    access
 41 Gi8/0/17            1214     0xDEF   8/240    up    access
 41 Gi8/0/17            1215     0xDF0   8/241    up    access

```

Table 12 describes the significant fields shown in the display.

Table 12 *show platform bridge Field Descriptions*

Field	Description
VLAN	The VLAN for which bridging is configured.
Interface	The WAN interface on which bridging is configured. This can be an ATM, Gigabit Ethernet, PoS, or serial interface.
CircuitId	The circuit ID. The range is from 0 to 65536.
LTL	The local target logic (LTL) of the interface. LTL is 13-bits long. The format is eee ssss pppppp (e=extended port bits, s=slot bits, p=port bits). Extended bits along with port bits identify the pseudoport and slot bits identifies the slot.
PseudoPort	In the case of FlexWAN, the port numbering is from 133 to 192 for Bay 0 and 197 to 256 for Bay 1. There are 60 ports per packet processing engine (PPE). For the SIP200, the pseudoports are in the range of 137 to 256.
State	State indicates the status of the physical interface on which bridging is configured. The state is either up or down. If the state is down, then there is a problem and debugging needs to be done.
Options	Options specify whether split-horizon is enabled on the WAN interface. This can be access, default, dot1q, or dot1q-tunnel.

Related Commands

Command	Description
show platform	Displays platform information.

show platform cfib

To display platform FIB information, use the **show platform cfib** command.

show platform cfib

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 display platform FIB information:

```
Router# show platform cfib
```

Related Commands	Command	Description
	platform cfib	Performs platform FIB configuration.

show platform cfm

To display connectivity fault management (CFM) commands, use the **show platform cfm** command in privileged EXEC mode.

```
show platform cfm { db | info | interface { gigabitethernet | port-channel | tengigabitethernet }
                  number }
```

Syntax Description	Parameter	Description
	db	Displays CFM DB details.
	info	Displays the CFM Platform Adaptation Layer (PAL) information.
	interface	Specifies the interface type.
	gigabitethernet	Specifies the Gigabit Ethernet interface.
	port-channel	Specifies the port channel interface.
	tengigabitethernet	Specifies the 10-Gigabit Ethernet interface.
	<i>number</i>	Interface number.

Command Default None

Command Modes Privileged EXEC (#)

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

Examples The following is sample output from the **show platform cfm info** command. The field descriptions are self-explanatory.

```
Router# show platform cfm info

CFM is disabled
CFM unicast MAC 00d0.2b6c.b103, CFM multicast MAC 0180.c200.0030, AEB multicast MAC
0100.0ccc.ccc0
CFM Ingress Control Packet System Statistics:
  Current software Rate Limit Setting: 1100 pkts/sec
  Statistics are collected in intervals of 3 seconds.
  Allow the first 3300 packets to pass each interval, drop thereafter
  Current Ingress Count in this interval: 0 pkts
  In this interval have we Exceeded Rate and Dropped pkts: NO
  For the last 3 intervals the maximum sample had 0 packets in one interval.
```

Related Commands	Command	Description
	show platform	Displays platform information.

show platform cts reflector interface

To display platform Cisco Trusted Security (CTS) reflector interface configuration, use the **show platform cts reflector interface** command.

```
show platform cts reflector interface { gigabitethernet number | tengigabitethernet number |
summary }
```

Syntax Description		
gigabitethernet <i>number</i>		Specifies GigabitEthernet interface number. Range is 1–6.
tengigabitethernet <i>number</i>		Specifies TenGigabitEthernet interface number. Range is 1–6.
summary		Specifies the platform CTS interface configuration summary.

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 display the platform CTS reflector interface configuration for tengigabitethernet interface number 4:

```
Router(config)# show platform cts reflector interface tengigabitethernet 4
```

Related Commands	Command	Description
	platform cts	Enables platform CTS configuration.

show platform datapath qos

To display QoS packet data path trace on the platform, use the **show platform datapath qos** command.

```
show platform datapath qos { cos | ingress-interface | last | lif | packet-data | pkt-length | recirc
| src-index }
```

Syntax Description

cos	Specifies the packet ingress CoS.
ingress-interface	Specifies the packet ingress interface (port, subinterface, service instance).
last	Specifies data from the last data path capture.
lif	Specifies packet ingress LIF from Eureka or shim header.
packet-data	Specifies packet header data specification.
pkt-length	Specifies the packet length.
recirc	Specifies the recirculated packet.
src-index	Specifies the packet ingress port source index.

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 display QoS packet data from the last data path capture:

```
Router# show platform datapath qos last
```

Related Commands

Command	Description
platform datapath qos	Enables QoS packet data path trace on the platform.

show platform eobc crs-delay

To display Ethernet out-of-band channel (EOBC) Carrier Router Service (CRS) delay on the platform, use the **show platform eobc crs-delay** command.

show platform eobc crs-delay

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 display EOBC CRS delay on the platform:

```
Router# show platform eobc crs-delay
```

Related Commands	Command	Description
	platform eobc crs-delay	Configures EOBC CRS delay on the platform.

show platform feature-manager consistency-check

To display platform-specific feature manager consistency checker configuration details, use the **show platform feature-manager consistency-check** command.

```
show platform feature-manager consistency-check { all | log | now { all | default-in | default-out
| dynamic | rbacl | static }
```

Syntax Description		
all		Displays all of the logs in memory from the consistency checker.
log		Displays logs from the most recent operation of consistency checker.
now		Processes the consistency checker now and displays the logs.
default-in		Processes it for the default non-permit results ingress direction.
default-out		Processes it for the default non-permit results egress direction.
dynamic		Processes it for the dynamic features.
rbacl		Processes it for the RBACL feature.
static		Processes it for the static features.

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 display the all of the platform-specific feature manager consistency checker configurations:

```
Router# show platform feature-manager consistency-check all
```

Related Commands	Command	Description
	clear platform feature-manager consistency-check all	Clears platform-specific feature manager consistency checker configurations.

show platform flow

To display NetFlow usage on the platform, use the **show platform flow usage** command.

```
show platform flow {aging | export {instance number | module number} | ip {count {instance
number | module number} | destination ip address | instance number | module number |
multicast | protocol number | source ip address} | ipv6 {count {instance number | module
number} | destination ip address | instance number | module number | multicast | protocol
number | source ip address} | layer2 {count {instance number | module number} | instance
number | module number} | multicast | protocol number | source ip address} | mpls {count
{instance number | module number} | instance number | module number} | table-contention
{aggregate {instance number | module number} | detailed {instance number | module
number} | summary {instance number | module number}} | usage {instance number | module
number}}
```

Syntax Description

aging	Specifies aging parameters.
export	Specifies export parameters.
ip	Specifies IP NetFlow entries.
ipv6	Specifies IPv6 NetFlow entries.
layer2	Specifies Layer 2 NetFlow entries.
mpls	Specifies MPLS NetFlow entries.
table-contention	Specifies NetFlow table contention.
aggregate	Provides information on aggregate NetFlow table contention.
detailed	Provides detailed information on NetFlow table contention.
summary	Provides a summary of NetFlow table contention.
usage	Specifies NetFlow table usage.
destination ip address	Specifies the destination IP address.
source ip address	Specifies the source IP address.
count	Specifies total number of NetFlow entries.
instance number	Specifies EARL instance number.
module number	Specifies 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 display the NetFlow usage on module 4:

```
Router# show platform flow usage module 4
```

Related Commands

Command	Description
platform flow	Enables NetFlow usage on the platform.

show platform flow export

To display the Yielding Netflow Data Export (NDE) parameters, use the **show platform flow export** command in Privileged EXEC mode.

show platform flow export module *module*

Syntax Description	module <i>module</i> Module and module number.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(50)SY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(50)SY	Support for this command was introduced.
Release	Modification				
12.2(50)SY	Support for this command was introduced.				

Examples

The following example displays the feature-related information for NDE:

```
Router(config)# show platform flow export module 4
Yielding NDE is enabled.
Supervisor CPU threshold = 50
Linecard CPU threshold   = 70

Module/Instance 1  :
-----
No of flows read and exported = 1802384
No of flows discarded        = 5230
No of capture+purge requests = 23049
No of purge-only requests    = 120

Module/Instance 5  :
-----
No of flows read and exported = 1
No of flows discarded        = 0
No of capture+purge requests = 13481
No of purge-only requests    = 11
lionel#
lionel#
lionel#sh pla flow exp mod 1
Yielding NDE is enabled.
Supervisor CPU threshold = 50
Linecard CPU threshold   = 70

Module/Instance 1  :
-----
No of flows read and exported = 1802384
No of flows discarded        = 5230

No of capture+purge requests = 23049
No of purge-only requests    = 120
```

Related Commands

Command	Description
flow hardware export	Configures NDE parameters.

show platform hardware acl accounting

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

```
show platform hardware acl accounting {index {number | range number}} | 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 | fcpa number | voabypassin number | voabypassout number | voafilterin number |
voafilterout number | voain number | voaout number}}
```

Syntax Description

index	Displays the accounting statistics.
number	Displays the accounting entry index. Range is 0–4095.
range <i>number</i>	Displays the particular accounting entry statistics. Range is 0–4095.
interface	Lists the various interfaces to choose ACL statistics for.
async <i>number</i>	Specifies the asynchronous interface number. Range is 1–999.
auto-template <i>number</i>	Specifies the auto-template interface number. Range is 1–999.
ctunnel <i>number</i>	Specifies the channel tunnel interface number. Range is 0–2147483647.
dialer <i>number</i>	Specifies the dialer interface number. Range is 0–255.
esconphy <i>number</i>	Specifies the EsconPhy interface number. Range is 1–6.
filter <i>number</i>	Specifies the filter interface number. Range is 1–6.
filtergroup <i>number</i>	Specifies the filter group interface number. Range is 1–6.
gigabitethernet <i>number</i>	Specifies the Gigabit Ethernet interface number. Range is 1–6.
longreachethernet <i>number</i>	Specifies the long-reach Ethernet interface number. Range is 1–6.
loopback <i>number</i>	Specifies the loopback interface number. Range is 1–2147483647.
mfr <i>number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink <i>number</i>	Specifies the multilink group interface number. Range is 1–2147483647.
null <i>number</i>	Specifies the null interface number. Range is 0–0.
port-channel <i>number</i>	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup <i>number</i>	Specifies the port group interface number. Range is 1–6.
pos-channel <i>number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom bus clock controller interface number. Range is 1–6.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.

virtual-tokenring <i>number</i>	Specifies the virtual Token Ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the Fibre Channel interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the ACL accounting statistics for VOA bypass-out interface number 4:

```
Router# show platform hardware acl accounting interface voabypassout 4
```

Related Commands	Command	Description
	platform hardware acl accounting	Configures platform hardware ACL accounting statistics for the available interfaces.

show platform hardware acl acct-xlt-tbl

To display ACL accounting tables, use the **show platform hardware acl acct-xlt-tbl** command.

```
show platform hardware acl acct-xlt-tbl {in {index {number | range number}} | out {index
{number | range number}}}
```

Syntax Description

in	Displays the accounting table entries that are available inside the ACL.
index	Displays the accounting table.
number	Displays the accounting table index.
range number	Displays the particular accounting table. Range is 0–255.
out	Displays the accounting table entries that are sent outside the ACL.

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 display the accounting XLT entries that are sent outside the ACL:

```
Router# show platform hardware acl acct-xlt-tbl out index
```

Related Commands

Command	Description
platform hardware acl acct-xlt-tbl	Configures platform hardware ACL accounting tables.

show platform hardware acl adj-rit

To display ACL TCAM adjacency entry information for various interfaces, use the **show platform hardware acl adj-rit** command.

```
show platform hardware acl adj-rit {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}}
```

Syntax	Description
interface	Specifies the type of interface.
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.
filter number	Specifies the filter interface number.
filtergroup number	Specifies the filter group interface number.
gigabitethernet number	Specifies the Gigabit Ethernet interface number.
longreachethernet number	Specifies the long-reach Ethernet interface number.
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.
pos-channel number	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock number	Specifies the telecom bus clock controller interface number.
tengigabitethernet number	Specifies the 10-Gigabit Ethernet interface number.
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.

control-plane <i>number</i>	Specifies the control plane interface number.
fcpa <i>number</i>	Specifies the Fibre Channel interface number.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number.
voain <i>number</i>	Specifies the VOA in interface number.
voaout <i>number</i>	Specifies the VOA out interface number.

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 display the adjacency entries for ACL asynchronous interface 4:

```
Router# show platform hardware acl adj-rit interface async 4
```

Related Commands

Command	Description
platform hardware acl adj-rit	Configures ACL TCAM adjacency entry information for various interfaces.

show platform hardware acl capmap tcam

To display hardware ACL cap map entries for TCAM, use the **show platform hardware acl capmap tcam** command.

```
show platform hardware acl capmap tcam {A {index number | module number} | B {index number | module number}}
```

Syntax Description		
A		Specifies entries in TCAM A.
B		Specifies entries in TCAM B.
index number		Specifies the cap map entry index number. Range is 0–2047.
module number		Specifies the module number.

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 display the TCAM A cap map entry index number 20:

```
Router# show platform hardware acl capmap tcam A Index 20
```

Related Commands	Command	Description
	platform hardware acl capmap tcam	Configures platform hardware ACL cap map entries for TCAM.

show platform hardware acl config-registers

To display hardware classify block registers by module number, use the **show platform hardware acl config-registers** command.

```
show platform hardware acl config-registers {module number}
```

Syntax Description	module number	Specifies the module number.
--------------------	---------------	------------------------------

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 display the hardware classify block register for module 4: Router# show platform hardware acl config-registers module 4
----------	---

Related Commands	Command	Description
	platform hardware acl config-registers	Configures platform hardware ACL classify block registers by module number.

show platform hardware acl destinfo

To display hardware ACL destination information, use the **show platform hardware acl destinfo** command.

```
show platform hardware acl destinfo { in { index number | module number } | out { index number | module number } | module number }
```

Syntax Description	Parameter	Description
	in	Specifies the inbound entries.
	<i>index number</i>	Displays the entry index number. Range is 0–511.
	<i>module number</i>	Displays the module number.
	out	Specifies the outbound entries.

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 display the ACL destination information for inbound entries in module 4:

```
Router# show platform hardware acl destinfo in module 4
```

Related Commands	Command	Description
	platform hardware acl destinfo	Configures platform hardware ACL destination information.

show platform hardware acl diagnostics

To display hardware ACL diagnostics reserved labels and indices by module number, use the **show platform hardware acl diagnostics** command.

```
show platform hardware acl diagnostics {module number}
```

Syntax Description	module number	Specifies the module number.
--------------------	---------------	------------------------------

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 display the hardware ACL diagnostics for module 4: Router# show platform hardware acl diagnostics module 4
----------	--

Related Commands	Command	Description
	platform hardware acl diagnostics	Configures platform hardware ACL diagnostics by module number.

show platform hardware acl entry

To display various ACL entries, use the **show platform hardware acl entry** command.

```
show platform hardware acl entry { compaction { module number } } | global-qos { in { arp { detail
| module number } | ip { detail | module number } | ipv6 { detail | module number } | mac { detail
| module number } | mpls { detail | module number } } | out { arp { detail | module number } | ip
{ detail | module number } | ipv6 { detail | module number } | mac { detail | module number } |
mpls { detail | module number } } | 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 |
cts-reflector number | fcpa number | voabypassin number | voabypassout number |
voafilterin number | voafilterout number | voain number | voaout number } } | rbacl { all
{ module number } | default { ip { module number } | ipv6 { module number } } | tcam { A { all
{ module number } | index number } | B { all { module number } | index number } } }
```

Syntax Description

compaction	Displays compaction entries.
module number	Specifies the module number.
global-qos	Displays global QoS entries.
in	Specifies inbound entries.
arp	Specifies the ARP protocol.
detail	Specifies the entry details.
ip	Specifies the IP protocol.
ipv6	Specifies the IPv6 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.
filter number	Specifies the filter interface number.
filtergroup number	Specifies the filter group interface number.
gigabitethernet number	Specifies the Gigabit Ethernet interface number.
longreachethernet number	Specifies the long-reach Ethernet interface number.
loopback number	Specifies the loopback interface number. Range is 1–2147483647.

mfr <i>number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink <i>number</i>	Specifies the multilink group interface number. Range is 1–2147483647.
null <i>number</i>	Specifies the null interface number. Range is 0–0.
port-channel <i>number</i>	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup <i>number</i>	Specifies the port group interface number.
pos-channel <i>number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom bus clock controller interface number.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.
virtual-tokenring <i>number</i>	Specifies the virtual Token Ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
control-plane <i>number</i>	Specifies the control plane interface number.
cts-reflector <i>number</i>	Specifies the CTS reflector interface number.
fcpa <i>number</i>	Specifies the Fibre Channel interface number.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number.
voain <i>number</i>	Specifies the VOA in interface number.
voaout <i>number</i>	Specifies the VOA out interface number.
rbacl	Displays RBACL entries.
all	Specifies all RBACL entries.
default	Specifies the default RBACL entry.
tcam A, tcam B	Displays entries by index for TCAM A, TCAM B.
index <i>number</i>	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 display the global QoS inbound ACL detailed entries for ARP protocol module 4:

```
Router# show platform hardware acl entry global-qos in arp detail module 4
```

Related Commands

Command	Description
<code>platform hardware acl entry</code>	Configures ACL entries.

show platform hardware acl ethertype-cam

To display hardware ACL Ethertype CAM table by module number, use the **show platform hardware acl ethertype-cam** command.

show platform hardware acl ethertype-cam { *module number* }

Syntax Description	module number	Specifies the module number.
---------------------------	----------------------	------------------------------

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	<p>This example shows how to display the hardware ACL Ethertype CAM table for module 4:</p> <pre>Router# show platform hardware acl ethertype-cam module 4</pre>	
-----------------	--	--

Related Commands	Command	Description
	platform hardware acl ethertype-cam	Configures platform hardware ACL Ethertype CAM table by module number.

show platform hardware acl hardware-hits

To display the TCAM hardware hits count, use the **show platform hardware acl hardware-hits** command.

```
show platform hardware acl hardware-hits {clear {module number} | show {module number}}
```

Syntax Description

clear	Displays the cleared hardware hits.
show	Displays the hardware hits since last clear.
module number	Specifies the module number.

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 display the TCAM hardware hits cleared for module 4:

```
Router# show platform hardware acl hardware-hits clear 4
```

Related Commands

Command	Description
platform hardware acl hardware-hits	Configures the TCAM hardware hits count.

show platform hardware acl initiate-lookup

To display ACL TCAM entries matching a pattern on available labels and interfaces, use the **show platform hardware acl initiate-lookup** command.

```
show platform hardware acl initiate-lookup {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 | fcpa number |
voabypassin number | voabypassout number | voafilterin number | voafilterout number |
voain number | voaout number} | label value tcam {A {arp {arp-rarp | arp_rarp_vld |
global_acl_fmt_match | l2_miss | mac_da_bcast | mac_sa | ofe mode | req-rpl | sender_ip |
src_snd_mac_same | src_tar_mac_same | target_ip | test} | ipv4 {acos | dst_port | first_seen
[ rp_bit ] | frag_flag | ip_da | ip_frag | ip_sa | l4_proto | l4op | module | src_dst_as_num |
src_port} | ipv6 {acos | dst_port | first_seen [ rp_bit ] | frag_flag | ip_da | ip_frag | ip_sa |
l4_proto | l4op | module | src_dst_as_num | src_port} | l2 {acos | ce_vlan | dscpl enc |
first_seen [ rp_bit ] | gpid | l2_miss | mac_da | mac_sa | module | vlan vlan_id} | mpls {acos
acos_gpid | exception | first_seen [ rp_bit ] | gpid_present | ip_hdr_vld | l2_miss | l4op |
module | mpls_exp | mpls_exp_from_null | mpls_exp_of_null | mpls_label | mpls_mcast |
mpls_stack | mpls_subtype | mpls_valid | u_key}} | B {arp {arp-rarp | arp_rarp_vld |
global_acl_fmt_match | l2_miss | mac_da_bcast | mac_sa | ofe mode | req-rpl | sender_ip |
src_snd_mac_same | src_tar_mac_same | target_ip | test} | ipv4 {acos | dst_port | first_seen
[ rp_bit ] | frag_flag | ip_da | ip_frag | ip_sa | l4_proto | l4op | module | src_dst_as_num |
src_port} | ipv6 {acos | dst_port | first_seen [ rp_bit ] | frag_flag | ip_da | ip_frag | ip_sa |
l4_proto | l4op | module | src_dst_as_num | src_port} | l2 {acos | ce_vlan | dscpl enc |
first_seen [ rp_bit ] | gpid | l2_miss | mac_da | mac_sa | module | vlan vlan_id} | mpls {acos
acos_gpid | exception | first_seen [ rp_bit ] | gpid_present | ip_hdr_vld | l2_miss | l4op |
module | mpls_exp | mpls_exp_from_null | mpls_exp_of_null | mpls_label | mpls_mcast |
mpls_stack | mpls_subtype | mpls_valid | u_key}}}
```

Syntax Description

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.
filter number	Specifies the filter interface number.
filtergroup number	Specifies the filter group interface number.
gigabitethernet number	Specifies the Gigabit Ethernet interface number.
longreachethernet number	Specifies the long-reach Ethernet interface number.
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.
pos-channel number	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock number	Specifies the telecom bus clock controller interface number.
tengigabitethernet number	Specifies the 10-Gigabit Ethernet interface number.
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.
voabypassin number	Specifies the VOA bypass-in interface number.
voabypassout number	Specifies the VOA bypass-out interface number.
voafilterin number	Specifies the VOA filter-in interface number.
voafilterout number	Specifies the VOA filter-out interface number.
voain number	Specifies the VOA in interface number.
voaout number	Specifies the VOA out interface number.
label value	Specifies the label value. Range is 1–8191.
tcam A, tcam B	Specifies TCAM A or TCAM B.
arp	Specifies the ARP protocol.
arp-rarp	Specifies ARP or RARP.
arp_rarp_vld	Specifies whether ARP or RARP is valid or not.
global acl fmt match	Specifies whether global ACL format matches or not.
l2_miss	Specifies whether the Layer 2 is missed.
mac_da_bcast	Specifies whether MAC destination address is broadcast.
mac_sa	Specifies the MAC source address.
ofe-mode	Specifies whether it is OFE mode.
req-rpl	Specifies whether it is reply or response.
sender_ip	Specifies the sender IP address.
src_snd_mac_same	Specifies whether the sender MAC is equal to Hbus source MAC.
src_tar_mac_same	Specifies whether the sender MAC is equal to Hbus target MAC.
target_ip	Specifies the target IP address.
test	Specifies test looping.
ipv4	Specifies the IPv4 protocol.
acos	Specifies the exception cause.
dst_port	Specifies the destination port.

first_seen	Specifies the first-seen bit for IFE.
rp_bit	(Optional) Specifies the from rp bit for OFE.
frag_flag	Specifies the fragmentation flag.
ip_da	Specifies the IP destination address.
ip_frag	Specifies the fragmentation bit for trailing fragments.
ip_sa	Specifies the IP source address.
l4_proto	Specifies the Layer 4 protocol code.
l4op	Specifies the Layer 4 op bits.
module	Specifies the module.
src_dst_as_num	Specifies the source or destination as number for OFE.
src_port	Specifies the source port number.
ipv6	Specifies the IPv6 protocol.
l2	Specifies the Layer 2 protocol.
ce_vlan	Specifies whether the CE VLAN is valid.
dscp	Specifies the DSCP.
enc	Specifies the encoding type.
gpid	Specifies whether the GPid is present.
mac_da	Specifies the MAC destination address.
mac_sa	Specifies the MAC source address.
mpls	Specifies the MPLS protocol.
acos_gpid	Specifies the GPid.
exception	Specifies if an exception exists.
gpid_present	Specifies whether the GPid is present.
ip_hdr_vld	Specifies whether the IP header is valid.
mpls_exp	Specifies the MPLS experimental value.
mpls_exp_from_null	Specifies whether the MPLS experimental value is from null label.
mpls_exp_of_null	Specifies whether the MPLS experimental value is of null label.
mpls_label	Specifies whether the MPLS label value exists.
mpls_mcast	Specifies MPLS multicast.
mpls_stack	Specifies whether the MPLS stack exists.
mpls_subtype	Specifies the MPLS subtype.
mpls_valid	Specifies whether the MPLS is valid.
u_key	Specifies the u key.

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 display the ACL TCAM entries matching a pattern on the asynchronous interface 4:

```
Router# show platform hardware acl initiate-lookup interface async 4
```

Related Commands	Command	Description
	platform hardware acl initiate-lookup	Configures ACL TCAM entries matching a pattern on available labels and interfaces.

show platform hardware acl label2sel tcam

To display label Layer 2 select entries for TCAM, use the **show platform hardware acl label2sel tcam** command.

```
show platform hardware acl label2sel tcam {A {index number} | B {index number}}
```

Syntax Description	A	B	index number
	Specifies label Layer 2 entries in TCAM A.	Specifies label Layer 2 entries in TCAM B.	Specifies the TCAM index number. Range is 0–8191.

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 display the TCAM A capmap entry index number 20:

```
Router# show platform hardware acl capmap tcam A Index 20
```

Related Commands	Command	Description
	platform hardware acl capmap tcam	Configures platform hardware ACL capmap entries for TCAM.

show platform hardware acl lou

To display the content of ACL logical operator units, use the **show platform hardware acl lou** command.

```
show platform hardware acl lou {index number | module number}
```

Syntax Description

index number	Specifies the LOU index number. Range is 0–103.
module number	Specifies the module number.

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 display the ACL logical operator units for module 4:

```
Router# show platform hardware acl lou module 4
```

Related Commands

Command	Description
platform hardware acl lou	Configures hardware logical operator units for ACLs.

show platform hardware acl status

To display hardware ACL status by module number, use the **show platform hardware acl status** command.

```
show platform hardware acl status {module number}
```

Syntax Description	module number	Specifies the module number.
--------------------	---------------	------------------------------

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 display the hardware ACL status for module 4: Router# show platform hardware acl status module 4
----------	--

Related Commands	Command	Description
	platform hardware acl status	Configures platform hardware ACL status by module number.

show platform hardware acl tcam

To display hardware ACL TCAM-related information, use the **show platform hardware acl tcam** command.

```
show platform hardware acl tcam { A { arp { accounting { module number } | module number | qos
  { module number } | security { module number } } | index number | ip { accounting { module
  number } | module number | qos { module number } | security { module number } } | ipv6
  { accounting { module number } | module number | qos { module number } | security { module
  number } } | l2v4 { accounting { module number } | module number | qos { module number } |
  security { module number } } | mac { accounting { module number } | module number | qos
  { module number } | security { module number } } | module number | mpls { accounting
  { module number } | module number | qos { module number } | security { module number } } }
```

```
show platform hardware acl tcam { B { arp { accounting { module number } | module number | qos
  { module number } | security { module number } } | index number | ip { accounting { module
  number } | module number | qos { module number } | security { module number } } | ipv6
  { accounting { module number } | module number | qos { module number } | security { module
  number } } | l2v4 { accounting { module number } | module number | qos { module number } |
  security { module number } } | mac { accounting { module number } | module number | qos
  { module number } | security { module number } } | module number | mpls { accounting
  { module number } | module number | qos { module number } | security { module number } } }
```

```
show platform hardware acl tcam { module number | result }
```

Syntax Description

A, B	Specifies TCAM A, TCAM B.
arp	Specifies the ARP protocol.
accounting	Specifies accounting entries.
module number	Specifies the module number.
qos	Specifies QoS entries.
security	Specifies security entries.
index number	Specifies entry index. Range is 0–131071.
ip	Specifies the IP protocol.
ipv6	Specifies the IPv6 protocol.
l2v4	Specifies the L2v4 protocol.
mac	Specifies the MAC protocol.
mpls	Specifies the MPLS protocol.
result	Specifies the result value.

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 display the TCAM A ARP accounting entries for module 4:

```
Router# show platform hardware acl tcam A arp accounting module 4
```

Related Commands

Command	Description
platform hardware acl tcam	Configures platform hardware ACL TCAM.

show platform hardware acl tcp-flags-tbl

To display information about hardware ACL TCP flags, use the **show platform hardware acl tcp-flags-tbl** command.

```
show platform hardware acl tcp-flags-tbl {detail | index number | module number}
```

Syntax Description	Parameter	Description
	detail	Displays TCP flags table details.
	index <i>number</i>	Specifies the TCP flag index number. Range is 0–255.
	module <i>number</i>	Specifies the TCP flag module number.

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 display the ACL TCP flags for module 4:

```
Router# show platform hardware acl tcp-flags-tbl module 4
```

Related Commands	Command	Description
	clear platform hardware acl tcp-flags-tbl	Clears hardware ACL TCP flags.

show platform hardware acl v6-extnhdr-tbl

To display information about hardware ACL v6 extension header table, use the **show platform hardware acl v6-extnhdr-tbl** command.

```
show platform hardware acl v6-extnhdr-tbl {detail | index number | module number}
```

Syntax Description	detail	Displays extension header table details.
	<i>index number</i>	Specifies the extension header table index number. Range is 0–127.
	<i>module number</i>	Specifies the extension header table module number.

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 display the hardware ACL v6 extension header table information for module 4:

```
Router# show platform hardware acl v6-extnhdr-tbl module 4
```

Related Commands	Command	Description
	platform hardware acl v6-extnhdr-tbl	Configures hardware ACL v6 extension header tables.

show platform hardware asicreg

To display hardware ASIC register-related information, use the **show platform hardware asicreg** command.

```
show platform hardware asicreg { dhanush {slot number} | hyperion | medusa | mii-phy |
palladium {get virtual_address | set virtual_address | all} | pentamak | ppc {all} | qchip |
rchip | revati | santa-ana | sculptor | scuti | solano | supersantaana | vishakha }
```

Syntax	Description
dhanush	Specifies the Dhanush ASIC.
slot number	Specifies the slot number.
hyperion	Specifies the Hyperion ASIC.
medusa	Specifies the Medusa ASIC.
mii-phy	Specifies the Mii-phy ASIC.
palladium	Specifies the Palladium I/O registers.
get virtual_address	Read Palladium I/O registers. Range is 0–4294967295.
set virtual_address	Write Palladium I/O registers. Range is 0–4294967295.
pentamak	Specifies the Pentamak ASIC.
ppc	Specifies the PPC I/O registers.
all	Specifies all I/O registers.
qchip	Specifies the Qchip ASIC.
rchip	Specifies the Rchip ASIC.
revati	Specifies the Revati ASIC.
santa-ana	Specifies the Santa-ana ASIC.
sculptor	Specifies the Sculptor ASIC.
scuti	Specifies the Scuti ASIC.
solano	Specifies the Solano ASIC.
supersantaana	Specifies the Supersantaana ASIC.
vishakha	Specifies the Vishakha ASIC.

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 display ASIC register information for the Dhanush ASIC, slot 4:

```
Router# show platform hardware asicreg dhanush slot 4
```

Related Commands

Command	Description
platform hardware asicreg	Configures platform hardware ASIC registers.

show platform hardware asic-versions

To display hardware ASIC versions by slot number, use the **show platform hardware asic-versions** command.

```
show platform hardware asic-versions {slot number}
```

Syntax Description	<i>slot number</i>	Specifies the slot number.
---------------------------	--------------------	----------------------------

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 display the hardware ASIC version for slot number 4: Router# show platform hardware asic-versions slot 4
-----------------	--

Related Commands	Command	Description
	platform hardware asic-versions	Configures platform hardware ASIC versions by slot number.

show platform hardware capacity

To display the capacities and utilizations for the hardware resources, use the **show platform hardware capacity** command in privileged EXEC mode.

show platform hardware capacity [*resource-type*]

Syntax Description	<i>resource-type</i>	(Optional) Hardware resource type; see the “Usage Guidelines” section for the valid values.
--------------------	----------------------	---

Defaults	None
----------	------

Command Modes	Privileged EXEC mode
---------------	----------------------

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

- Usage Guidelines**
- The valid values for *resource-type* are as follows:
- **acl**—Displays the capacities and utilizations for ACL or QoS TCAM resources.
 - **cpu**—Displays the capacities and utilizations for CPU resources.
 - **eobc**—Displays the capacities and utilizations for Ethernet out-of-band channel resources.
 - **fabric**—Displays the capacities and utilizations for switch fabric resources.
 - **flash**—Displays the capacities and utilizations for flash or NVRAM resources.
 - **forwarding**—Displays the capacities and utilizations for Layer 2 and Layer 3 forwarding resources.
 - **ibc**—Displays the capacities and utilizations for interboard communication resources.
 - **interface**—Displays the capacities and utilizations for interface resources.
 - **monitor**—Displays the capacities and utilizations for SPAN resources.
 - **multicast**—Displays the capacities and utilizations for Layer 3 multicast resources.
 - **netflow**—Displays the capacities and utilizations for NetFlow resources.
 - **pfc**—Displays the capacities and utilizations for all the PFC resources including Layer 2 and Layer 3 forwarding, NetFlow, CPU rate limiters, and ACL or QoS TCAM resources.
 - **power**—Displays the capacities and utilizations for power resources.
 - **qos**—Displays the capacities and utilizations for QoS policer resources.
 - **rate-limit**—Displays the capacities and utilizations for CPU rate-limiter resources.
 - **rewrite-engine**—Displays the packet drop and performance counters of the central rewrite engine on supervisor engines and line cards. For detailed information, see the **show platform hardware capacity rewrite-engine** command documentation.

- **system**—Displays the capacities and utilizations for system resources.
- **vlan**—Displays the capacities and utilizations for VLAN resources.

The **show platform hardware capacity cpu** command displays the following information:

- CPU utilization for the last 5 seconds (busy time and interrupt time), the percentage of the last 1-minute average busy time, and the percentage of the last 5-minute average busy time.
- Processor memory total available bytes, used bytes, and percentage used.
- I/O memory total available bytes, used bytes, and percentage used.

The **show platform hardware capacity eobc** command displays the following information:

- Transmit and receive rate
- Packets received and packets sent
- Dropped received packets and dropped transmitted packets

The **show platform hardware capacity forwarding** command displays the following information:

- The total available entries, used entries, and used percentage for the MAC tables.
- The total available entries, used entries, and used percentage for the FIB TCAM tables. The display is done per-protocol base.
- The total available entries, used entries, and used percentage for the adjacency tables. The display is done for each region in which the adjacency table is divided.
- The created entries, failures, and resource usage percentage for the NetFlow TCAM and ICAM tables.
- The total available entries and mask, used entries and mask, reserved entries and mask, and entries and mask used percentage for the ACL/QoS TCAM tables. The output displays the available, used, reserved, and used percentage of the labels. The output displays the resource of other hardware resources that are related to the ACL/QoS TCAMs (such as available, used, reserved, and used percentage of the LOU, ANDOR, and ORAND).
- The available, used, reserved, and used percentage for the CPU rate limiters.

The **show platform hardware capacity interface** command displays the following information:

- Tx/Rx drops—Displays the sum of transmit and receive drop counters on each online module (aggregate for all ports) and provides the port number that has the highest drop count on the module.
- Tx/Rx per port buffer size—Summarizes the port-buffer size on a per-module basis for modules where there is a consistent buffer size across the module.

The **show platform hardware capacity monitor** command displays the following SPAN information:

- The maximum local SPAN sessions, maximum RSPAN sessions, maximum ERSPAN sessions, and maximum service module sessions.
- The local SPAN sessions used or available, RSPAN sessions used or available, ERSPAN sessions used or available, and service module sessions used or available.

The **show platform hardware capacity multicast** command displays the following information:

- Multicast Replication Mode – Ingress and egress IPv4 and IPv6 modes.
- The MET table usage that indicates the total used and the percentage used for each module in the system.
- The bidirectional PIM DF table usage that indicates the total used and the percentage used.

The **show platform hardware capacity system** command displays the following information:

- PFC operating mode (PFC version: PFC3A, PFC3B, unknown, and so forth)
- Supervisor engine redundancy mode (RPR, RPR+, SSO, none, and so forth)
- Module-specific switching information, including the following information:
 - Part number (WS-SUP720-BASE, WS-X6548-RJ-45, and so forth)
 - Series (supervisor engine, fabric, CEF720, CEF256, dCEF256, or classic)
 - CEF mode (central CEF, dCEF)

The **show platform hardware capacity vlan** command displays the following VLAN information:

- Total VLANs
- VTP VLANs that are used
- External VLANs that are used
- Internal VLANs that are used
- Free VLANs

Examples

This example shows how to display CPU capacity and utilization information for the route processor, the switch processor, and the LAN module in the Cisco 7600 series router:

```
Router# show platform hardware capacity cpu
CPU Resources
CPU utilization: Module           5 seconds      1 minute      5 minutes
                   1 RP             0% / 0%         1%            1%
                   1 SP             5% / 0%         5%            4%
                   7                 69% / 0%       69%          69%
                   8                 78% / 0%       74%          74%
Processor memory: Module  Bytes:      Total          Used           %Used
                   1 RP             176730048     51774704       29%
                   1 SP             192825092     51978936       27%
                   7                 195111584     35769704       18%
                   8                 195111584     35798632       18%
I/O memory: Module  Bytes:      Total          Used           %Used
                   1 RP             35651584      12226672       34%
                   1 SP             35651584      9747952        27%
                   7                 35651584      9616816        27%
                   8                 35651584      9616816        27%

Router#
```

This example shows how to display EOBC-related statistics for the route processor, the switch processor, and the DFCs in the Cisco 7600 series router:

```
Router# show platform hardware capacity eobc
EOBC Resources
Module           Packets/sec      Total packets      Dropped packets
1 RP   Rx:         61              108982              0
       Tx:         37              77298               0
1 SP   Rx:         34              101627              0
       Tx:         39              115417              0
7      Rx:         5               10358               0
       Tx:         8               18543               0
8      Rx:         5               12130               0
       Tx:        10              20317               0

Router#
```

This example shows how to display the current and peak switching utilization:

```
Router# show platform hardware capacity fabric
Switch Fabric Resources
  Bus utilization: current is 100%, peak was 100% at 12:34 12mar45
  Fabric utilization:
    ingress
      Module channel speed current peak
      1 0 20G 100% 100% 12:34 12mar45
      1 1 20G 12% 80% 12:34 12mar45
      4 0 20G 12% 80% 12:34 12mar45
      13 0 8G 12% 80% 12:34 12mar45
    egress
      current peak
      100% 100% 12:34 12mar45
      12% 80% 12:34 12mar45
      12% 80% 12:34 12mar45
      12% 80% 12:34 12mar45
Router#
```

This example shows how to display information about the total capacity, the bytes used, and the percentage that is used for the flash or NVRAM resources present in the system:

```
Router# show platform hardware capacity flash
Flash/NVRAM Resources
  Usage: Module Device Bytes: Total Used %Used
        1 RP bootflash: 31981568 15688048 49%
        1 SP disk0: 128577536 105621504 82%
        1 SP sup-bootflash: 31981568 29700644 93%
        1 SP const_nvram: 129004 856 1%
        1 SP nvram: 391160 22065 6%
        7 dfc#7-bootflash: 15204352 616540 4%
        8 dfc#8-bootflash: 15204352 0 0%
Router#
```

This example shows how to display the capacity and utilization of the EARLs present in the system:

```
Router# show platform hardware capacity forwarding
L2 Forwarding Resources
  MAC Table usage: Module Collisions Total Used %Used
                  6 0 65536 11 1%
  VPN CAM usage: Total Used %Used
                 512 0 0%

L3 Forwarding Resources
  FIB TCAM usage: Total Used %Used
    72 bits (IPv4, MPLS, EoM) 196608 36 1%
    144 bits (IP mcast, IPv6) 32768 7 1%
  detail: Protocol Used %Used
          IPv4 36 1%
          MPLS 0 0%
          EoM 0 0%
          IPv6 4 1%
          IPv4 mcast 3 1%
          IPv6 mcast 0 0%
  Adjacency usage: Total Used %Used
                  1048576 175 1%

Forwarding engine load:
  Module pps peak-pps peak-time
  6 8 1972 02:02:17 UTC Thu Apr 21 2005

Netflow Resources
  TCAM utilization: Module Created Failed %Used
                  6 1 0 0%
  ICAM utilization: Module Created Failed %Used
                  6 0 0 0%

Flowmasks: Mask# Type Features
IPv4: 0 reserved none
IPv4: 1 Intf FulNAT_INGRESS NAT_EGRESS FM_GUARDIAN
IPv4: 2 unused none
IPv4: 3 reserved none
IPv6: 0 reserved none
IPv6: 1 unused none
```

```

IPv6:      2  unused  none
IPv6:      3  reserved none

CPU Rate Limiters Resources
Rate limiters:      Total      Used      Reserved      %Used
Layer 3             9         4         1             44%
Layer 2             4         2         2             50%

ACL/QoS TCAM Resources
Key: ACLent - ACL TCAM entries, ACLmsk - ACL TCAM masks, AND - ANDOR,
QoSent - QoS TCAM entries, QoSmsk - QoS TCAM masks, OR - ORAND,
Lbl-in - ingress label, Lbl-eg - egress label, LOUsrc - LOU source,
LOUdst - LOU destination, ADJ - ACL adjacency
Module ACLent ACLmsk QoSent QoSmsk Lbl-in Lbl-eg LOUsrc LOUdst AND OR ADJ
6         1%      1%      1%      1%      1%      1%      0%      0%      0%      0%      1%
Router#

```

This example shows how to display the interboard communication resources:

```

Router# show platform hardware capacity ibc
IBC Resources
Module      Packets/sec      Total packets      Dropped packets
1  RP      Rx:              3          5001419             0
          Tx:              1          1943884             0
Router#

```

This example shows how to display the interface resources:

```

Router# show platform hardware capacity interface
Interface Resources
Interface drops:
Module      Total drops:      Tx      Rx      Highest drop port:      Tx      Rx
9           0              0          2          0 48

Interface buffer sizes:
Module      Bytes:      Tx buffer      Rx buffer
1           12345      12345          12345
5           12345      12345          12345
Router#

```

This example shows how to display SPAN information:

```

Router# show platform hardware capacity monitor
SPAN Resources
Source sessions: 2 maximum, 0 used
Type      Used
Local     0
RSPAN source 0
ERSPAN source 0
Service module 0
Destination sessions: 64 maximum, 0 used
Type      Used
RSPAN destination 0
ERSPAN destination (max 24) 0
Router#

```

This example shows how to display the capacity and utilization of resources for Layer 3 multicast functionality:

```

Router# show platform hardware capacity multicast
L3 Multicast Resources
IPv4 replication mode: ingress
IPv6 replication mode: ingress
Bi-directional PIM Designated Forwarder Table usage: 4 total, 0 (0%) used
Replication capability: Module      IPv4      IPv6
5           egress      egress
9           ingress      ingress
MET table Entries: Module      Total      Used      %Used

```



```

Router#                               5                               65526       6       0%

```

This example shows how to display information about the system power capacities and utilizations:

```

Router# show platform hardware capacity power
Power Resources
  Power supply redundancy mode: administratively combined
                                operationally combined
  System power: 1922W, 0W (0%) inline, 1289W (67%) total allocated
  Powered devices: 0 total
Router#

```

This example shows how to display the capacity and utilization of QoS policer resources per EARL in the Cisco 7600 series router:

```

Router# show platform hardware capacity qos
QoS Policer Resources
Aggregate policers: Module          Total      Used      %Used
                    1              1024      102       10%
                    5              1024        1         1%
Microflow policer configurations: Module  Total      Used      %Used
                                        1          64        32        50%
                                        5          64         1         1%
Router#

```

This example shows how to display information about the key system resources:

```

Router# show platform hardware capacity system
System Resources
  PFC operating mode: PFC3BXL
  Supervisor redundancy mode: administratively rpr-plus, operationally rpr-plus
  Switching Resources: Module  Part number      Series      CEF mode
                        5      WS-SUP720-BASE  supervisor  CEF
                        9      WS-X6548-RJ-45  CEF256     CEF
Router#

```

This example shows how to display VLAN information:

```

Router# show platform hardware capacity vlan
VLAN Resources
  VLANs: 4094 total, 10 VTP, 0 extended, 0 internal, 4084 free
Router#

```

Related Commands

Command	Description
show msfc	Displays MSFC information.
show platform	Displays platform information.
show platform hardware capacity rewrite-engine	Displays the packet drop and performance counters of the central rewrite engine on supervisor engines and line cards.

show platform hardware capacity rewrite-engine

To display the packet drop and performance counters of the central rewrite engine on supervisor engines and line cards, use the **show platform hardware capacity rewrite-engine** command in privileged EXEC mode.

```
show platform hardware capacity rewrite-engine {drop | performance} [slot number]
[rate [sample_interval]] [details]
```

Syntax Description	drop	Displays the central rewrite engine drop counter values.
	performance	Displays the central rewrite engine current performance counter values or the performance rate.
	slot number	(Optional) Displays the counter values for the module in the specified slot. If no slot is specified, the counters are displayed for each slot.
	rate sample_interval	(Optional) Displays the drop rate or rewrite rate for a sample interval in msec between 1 and 1000. The default interval is 50 msec.
	details	(Optional) Displays each individual drop counter with its name and register ID number. This keyword is not available with the performance keyword.

Defaults If the sample interval is not specified, the default interval is 50 msec.

Command Modes Privileged EXEC

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

Usage Guidelines In the **show platform hardware capacity rewrite-engine performance** command output, a value of N/A indicates that the slot or channel has a rewrite engine, but does not support performance counters.

Examples This example shows how to display the packet drop counters of the central rewrite engine in all installed supervisor engines and line cards:

```
Router# show platform hardware capacity rewrite-engine drop
```

```
slot channel  packet drops      total overruns
-----+-----+-----+
1      0          0                0
5      0      15440040         22
7      0          44                0
7      1          0                0
```

This example shows how to display a detailed report of the packet drop counters of the module in slot 1:

Router# **show platform hardware capacity rewrite-engine drop slot 1 details**

slot	channel	drop_id	description	packet drops	total overruns
1	0	0x5ED	DROP NON BPDU	0	0
1	0	0x5EB	DROP BPDU	0	0
1	1	0x5ED	DROP NON BPDU	0	0
1	1	0x5EB	DROP BPDU	0	0

This example shows how to display the packet drop counters of the module in slot 5 over the default sample interval of 50 msec:

Router# **show platform hardware capacity rewrite-engine drop slot 5 rate**

slot	channel	drop rate [pps]	overrun [Y/N]
5	0	120079	Y

This example shows how to display the packet drop counters of the module in slot 5 over a sample interval of 20 msec:

Router# **show platform hardware capacity rewrite-engine drop slot 5 rate 20**

slot	channel	drop rate [pps]	overrun [Y/N]
5	0	180000	N

This example shows how to display the performance counters of the central rewrite engine in all installed supervisor engines and line cards:

Router# **show platform hardware capacity rewrite-engine performance**

slot	channel	perf_id	description	packets	total overruns
1	0	0x235	FAB RX 0	12870	0
1	0	0x237	FAB RX 1	0	0
1	0	0x27B	FAB TX 0	164	0
1	0	0x27F	FAB TX 1	0	0
1	0	0x350	REPLICATION ML3	0	0
1	0	0x351	REPLICATION ML2	0	0
1	0	0x352	RECIRC L2	0	0
1	0	0x353	RECIRC L3	0	0
1	0	0x34C	SPAN TX 0	0	0
1	0	0x34D	SPAN TX 1	0	0
1	0	0x34E	SPAN RX 0	0	0
1	0	0x34F	SPAN RX 1	0	0
1	0	0x354	SPAN TERMINATION	0	0
1	1	0x235	FAB RX 0	106065	0
1	1	0x237	FAB RX 1	0	0
1	1	0x27B	FAB TX 0	180806	0
1	1	0x27F	FAB TX 1	0	0
1	1	0x350	REPLICATION ML3	0	0
1	1	0x351	REPLICATION ML2	0	0
1	1	0x352	RECIRC L2	0	0
1	1	0x353	RECIRC L3	0	0
1	1	0x34C	SPAN TX 0	0	0
1	1	0x34D	SPAN TX 1	0	0
1	1	0x34E	SPAN RX 0	201	0
1	1	0x34F	SPAN RX 1	90201	0
1	1	0x354	SPAN TERMINATION	0	0
4	0	N/A			
5	0	0xBE	FAB RX 0	181496	0

5	0	0xC0	FAB RX 1	0	0
5	0	0x112	FAB TX 0	992089	0
5	0	0x116	FAB TX 1	0	0
5	0	0x299	REPLICATION ML3	0	0
5	0	0x29A	REPLICATION ML2	0	0
5	0	0x29B	RECIRC L2	0	0
5	0	0x29C	RECIRC L3	0	0
5	0	0x295	SPAN TX 0	91166	0
5	0	0x296	SPAN TX 1	91313	0
5	0	0x297	SPAN RX 0	1	0
5	0	0x298	SPAN RX 1	1	0
5	0	0x29D	SPAN TERMINATION	0	0

This example shows how to display the performance counters of the module in slot 5:

Router# **show platform hardware capacity rewrite-engine performance slot 5**

slot	channel	perf_id	description	packets	total overruns
5	0	0xBE	FAB RX 0	1330	0
5	0	0xC0	FAB RX 1	0	0
5	0	0x112	FAB TX 0	715253	0
5	0	0x116	FAB TX 1	0	0
5	0	0x299	REPLICATION ML3	0	0
5	0	0x29A	REPLICATION ML2	0	0
5	0	0x29B	RECIRC L2	0	0
5	0	0x29C	RECIRC L3	0	0
5	0	0x295	SPAN TX 0	1022	0
5	0	0x296	SPAN TX 1	1152	0
5	0	0x297	SPAN RX 0	1	0
5	0	0x298	SPAN RX 1	1	0
5	0	0x29D	SPAN TERMINATION	0	0

This example shows how to display the performance counters of the module in slot 5 over the default sample interval of 50 msec:

Router# **show platform hardware capacity rewrite-engine performance slot 5 rate**

slot	channel	perf_id	description	packet rate[pps]	overrun [Y/N]
5	0	0xBE	FAB RX 0	11680	N
5	0	0xC0	FAB RX 1	0	N
5	0	0x112	FAB TX 0	11680	N
5	0	0x116	FAB TX 1	0	N
5	0	0x299	REPLICATION ML3	0	N
5	0	0x29A	REPLICATION ML2	0	N
5	0	0x29B	RECIRC L2	0	N
5	0	0x29C	RECIRC L3	0	N
5	0	0x295	SPAN TX 0	5840	N
5	0	0x296	SPAN TX 1	5840	N
5	0	0x297	SPAN RX 0	0	N
5	0	0x298	SPAN RX 1	0	N
5	0	0x29D	SPAN TERMINATION	0	N

Related Commands

Command	Description
clear platform hardware capacity rewrite-engine counter	Clears the packet drop and performance counters of the central rewrite engine on supervisor engines and line cards.

show platform hardware cbl

To display hardware CBL by slot number, use the **show platform hardware cbl** command.

```
show platform hardware cbl {slot number}
```

Syntax Description	<i>slot number</i>	Specifies the module number.
---------------------------	--------------------	------------------------------

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 display the hardware CBL for slot 4:
-----------------	--

```
Router# show platform hardware cbl slot 4
```

Related Commands	Command	Description
	platform hardware cbl	Configures platform hardware CBL by slot number.

show platform hardware cef mpls detail

To display MPLS CEF detail information use the **show platform hardware cef mpls detail** command in privileged EXEC mode.

```
show platform hardware cef mpls detail [earl earl-id | module mod-num] group {ip-addr [detail | verbose]}
```

Syntax Description	
earl <i>earl-id</i>	(Optional) Displays the CEF detail for the EARL; valid values are 1 or 2.
module <i>mod-num</i>	(Optional) Displays the CEF detail for a module; valid values are 1 through 6.
group	Shows the hardware entries for a group.
<i>ip-addr</i> detail	Shows the hardware entry details.
<i>ip-addr</i> verbose	Shows the hardware entry verbose details.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines The **show platform hardware cef mpls detail** command displays detailed information about MPLS adjacency entries. For each adjacency, use the **show platform hardware cef adjacencies entry** command to display the MPLS adjacency information.

Examples This example shows how to display the MPLS CEF hardware details for EARL 1:

```
Router# show platform hardware multicast routing ip group 226.1.1.1 detail
show platform hardware cef mpls detail earl 1
Codes: M - mask entry, V - value entry, A - adjacency index, NR- no_route bit
LS - load sharing count, RI - router_ip bit, DF: default bit
CP - copy_to_cpu bit, AS: dest_AS_number, DGTv - dgt_valid bit
DGT: dgt/others value, LS: load sharing count on eos condition
EE: EOS enable, NW: num swap paths, NP: num push paths

Format:MPLS (valid class vpn_tbid vpn_vld Label0 M EoS Lif/Label1
M(52740 ): 1 F 3FFF 1 FFFF 0 1 0
V(52740 ): 1 2 0 1 1 0 0 0
(A:213012, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:0, DGT:0)
M(52742 ): 1 F 3FFF 1 FFFF 0 1 0
V(52742 ): 1 2 0 1 1 0 1 0
(A:78089 , LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:0, DGT:0)
M(52822 ): 1 F 3FFF 1 FFFF 0 1 0
V(52822 ): 1 2 0 1 21 0 1 0
```

```

(A:213013, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:0, DGT:0)
M(52830 ): 1 F 3FFF 1 FFFF 0 1 0
V(52830 ): 1 2 0 1 23 0 1 0
(A:213017, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:0, DGT:0)
M(52834 ): 1 F 3FFF 1 FFFF 0 1 0
V(52834 ): 1 2 0 1 24 0 1 0
Router#

```

Related Commands

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

show platform hardware cef adjacencies entry

To display a single adjacency entry index, use the **show platform hardware cef adjacencies entry** command in privileged EXEC mode

show platform hardware cef adjacencies entry *entry-num*

Syntax Description	<i>entry-num</i>	Displays the adjacency index; valid values are 0 through 1048575.
---------------------------	------------------	---

Defaults	None
-----------------	------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Examples This example shows how to display the index for CEF adjacency 45:

```
Router# show platform hardware cef adjacencies entry 45
Index: 45 -- Valid entry (valid = 1) --
```

Adjacency fields:

adj_stats = EN	fwd_stats = EN	format = IP
rdt = OFF	elif = 0x2D	vpn = 0x3FFF

RIT fields: The entry has a Recirc. Format

decr_ttl=NO	l2_fwG=YES	ccc = 4	add_shim_hdr = NO
-------------	------------	---------	-------------------

Statistics: Packets = 0
Bytes = 0

Router#

Related Commands	Command	Description
	debug platform software multicast routing	Displays information about multicast errors.
	platform software met profile	Configures the number of blocks for each block size of your MET profile.
	show platform hardware cef mpls detail	Displays MPLS CEF detail information.

Command	Description
show platform hardware met read	Displays platform hardware MET table entries.
show platform hardware multicast routing	Matches and displays multicast routing group IP addresses.
show platform software met detail	Displays software routing for the MET.

show platform hardware cef tcam

To display platform hardware Cisco Express Forwarding (CEF) Forwarding Information Base (FIB) Ternary Content Addressable Memory (TCAM), use the **show platform hardware cef** command.

```
show platform hardware cef tcam {ecc [detail [earl earl-id] | module module-num] | earl earl-id] |
module module-num] | hit [detail [earl earl-id] | module module-num] | earl earl-id] | module
module-num] | keys [count | exception ] | memory usage | segment [detail [earl earl-id] |
module module-num] | earl earl-id] | module module-num] | select [detail [earl earl-id] |
module module-num] | earl earl-id] | module module-num] | shadow [detail [earl earl-id] |
module module-num] | earl earl-id] | module module-num] | timing [detail [earl earl-id] |
module module-num] | earl earl-id] | module module-num] | utilization [detail [earl earl-id] |
module module-num] | earl earl-id] | module module-num] | earl earl-id] | module module-num]
```

Syntax	Description
ecc	Displays error checking and correction (ECC) information.
detail	(Optional) Displays detailed information.
earl earl-id	(Optional) Displays earl-id content.
module module-num	(Optional) Displays information for a specific module.
hit	Displays last hit on the FIB TCAM information.
keys	Displays keys information.
count	(Optional) Displays keys count information.
exception	(Optional) Displays keys exception information.
memory usage	Displays memory usage.
segment	Displays segment distribution.
select	Displays bit-select information.
shadow	Displays the shadow copy.
timing	Displays timing utilization.
utilization	Displays segment utilization.

Defaults None

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(33)SX	Support for this command was introduced.
	15.1(1)SY	Added ecc , key , memory , segment , select , shadow , timing , and utilization keywords.

Examples

This example shows how to display the hardware CEF TCAM key exception:

```
Router(config)# show platform hardware cef tcam keys exception
```

Priorities in exception:

Class	ID	Pri (>=)	Max	Key-Cnt	Pri-Cnt
IPv4	0	16	35	35085	
IPv4-Mcast	1	68	68	0	
MPLS	2	17	17	0	
EOMPLS	3	19	19	0	
MPLS-VPN	4	9	9	0	
Diags	5	5	5	0	
IPv6-Local	6	390	390	0	
IPv6-Mcast	7	261	261	0	
IPv6-Global	8	244	390	1051	
VPLSv4-Mcast	9	69	69	0	
VPLSv6-Mcast	10	261	261	0	

Keys in each Pri in exception:

Class	ID	Pri	XCP	Pri-Cnt
IPv4	0	16		4096
.	.	17		15507
.	.	18		7753
.	.	19		3876
.	.	20		1939
.	.	21		969
.	.	22		484
.	.	23		243
.	.	24		121
.	.	25		60
.	.	26		34
.	.	30		2
.	.	34		1
IPv6-Global	8	244		129
.	.	245		126
.	.	246		118
.	.	247		114
.	.	248		111
.	.	249		109

.	.	250	109
.	.	251	107
.	.	252	64
.	.	253	32
.	.	254	16
.	.	255	8
.	.	256	4
.	.	257	2
.	.	389	1
.	.	390	1

Spanslogic#show platform hardware cef tcam memory usage

Buffer allocation summary:

Id	Data Size	Page Size	Total Count	Total Size	Used Count	Used Size	Free Count	Free Size	Type
0	0	0	0	0	0	0	0	0	Void
1	80	80	0	0	0	0	0	0	Bsort
2	2076	65536	279	576K	0	0	279	565K	Bsort Node
3	3456	65536	288	1.00M	20	39744	268	904K	Bsort Stat
4	60	65536	2184	128K	1697	99.4K	487	29220	Wsort Seg
5	104	65536	630	65536	17	1768	613	63752	Wsort Win
6	1024	65536	384	384K	17	17408	367	367K	Wsort Avail
7	3644	3644	3	10932	3	10932	0	0	Group
8	324	8192	25	8192	20	6480	5	1620	Group Entry
9	0	0	2	20480	2	20480	0	0	SE Block
10	4104	65536	3660	15.2M	2814	11.1M	846	3.31M	SE Slice
11	52	65536	2520	128K	1697	88244	823	42796	SE Seg
12	68	65536	18297	1.18M	0	0	18297	1.18M	SE Rec
13	0	0	0	0	0	0	0	0	SE Pri
14	48	65536	619k	28.3M	587k	26.8M	32320	1.47M	Key
15	8	65536	0	0	0	0	0	0	Bit 64
16	12	65536	1.20m	13.7M	1.13m	13.2M	63352	742K	Bit 96
17	16	65536	0	0	0	0	0	0	Bit 128
18	20	65536	39312	768K	36634	715K	2678	53560	Bit 160
19	24	24	0	0	0	0	0	0	Bit 192
20	28	28	0	0	0	0	0	0	Bit 224
21	32	65536	8192	256K	5628	175K	2564	82048	Bit 256

```

22 36 65536 0 0 0 0 0 0 Bit 288
23 40 65536 1638 65536 98 3920 1540 61600 Bit 320
24 44 44 0 0 0 0 0 0 Bit 352
25 48 48 0 0 0 0 0 0 Bit 384
26 52 52 0 0 0 0 0 0 Bit 416
27 56 56 0 0 0 0 0 0 Bit 448
28 60 65536 0 0 0 0 0 0 Bit 480
29 64 64 0 0 0 0 0 0 Bit 512
30 68 68 0 0 0 0 0 0 Bit 544
31 72 72 0 0 0 0 0 0 Bit 576
32 76 76 0 0 0 0 0 0 Bit 608
33 80 65536 0 0 0 0 0 0 Bit 640
34 84 84 0 0 0 0 0 0 Bit 672
35 88 88 0 0 0 0 0 0 Bit 704
* * * 1.89m 61.9M 1.77m 52.7M 124k 8.81M Total

```

Router(config)#

This example shows how to display the hardware CEF TCAM timing information:

Router(config)# **show platform hardware cef tcam timing**

```

(0) Groom Clock: 182us (Min) << 71ms (Avg) << 404ms (Max) = 09.19s (Tot)
 5.28ms 1.16ms 10ms 38ms 3.43ms 10ms 166ms 223ms
 5.06ms 960us 9.34ms 37ms 1.79ms 96ms 110ms 155ms
 4.72ms 1.06ms 8.90ms 34ms 813us 4.14ms 110ms 138ms
 4.12ms 755us 6.81ms 32ms 305us 75ms 28ms 237ms
 3.90ms 690us 6.13ms 30ms 228us 50ms 247ms 199ms
 3.67ms 529us 5.81ms 28ms 274us 94ms 217ms 63ms
 3.38ms 506us 3.68ms 25ms 1.73ms 269ms 218ms 96ms
 3.14ms 400us 2.94ms 23ms 279us 119ms 277ms 66ms
 2.94ms 351us 3.63ms 20ms 115ms 163ms 346ms 94ms
 2.87ms 306us 2.75ms 18ms 46ms 404ms 316ms 35ms
 2.76ms 291us 1.18ms 16ms 156ms 351ms 154ms 84ms
 3.30ms 275us 794us 13ms 87ms 319ms 220ms 5.51ms
 5.20ms 202us 736us 11ms 8.52ms 85ms 220ms 203ms
 2.77ms 190us 39ms 9.58ms 112ms 229ms 189ms 191ms
 1.58ms 182us 39ms 7.52ms 73ms 180ms 172ms 216ms
 1.84ms 11ms 38ms 5.63ms 90ms 188ms 227ms 1.27ms

(1) Add Clock: 11us (Min) << 13us (Avg) << 107us (Max) = 1.78ms (Tot)
11us 11us 11us 12us 11us 12us 12us 12us
11us 12us 12us 11us 11us 11us 11us 12us
12us 11us 12us 12us 11us 12us 12us 12us
12us 12us 12us 12us 11us 12us 12us 13us

```

```

11us    12us    12us    12us    11us    11us    11us    12us
12us    12us    12us    12us    11us    12us    12us    12us
12us    12us    11us    12us    11us    11us    11us    12us
11us    11us    12us    11us    11us    12us    12us    12us
11us    12us    11us    11us    11us    12us    11us    11us
12us    12us    12us    11us    11us    11us    11us    40us
107us   12us    12us    12us    12us    12us    12us    41us
12us    11us    11us    12us    12us    12us    11us    40us
12us    12us    11us    12us    12us    11us    11us    40us
11us    11us    12us    12us    12us    12us    11us    40us
12us    12us    12us    12us    12us    11us    12us    40us
12us    12us    11us    11us    11us    12us    12us    40us
Router(config)#

```

This example shows how to display the hardware CEF TCAM utilization information:

```
Router(config)# show platform hardware cef tcam utilization
```

Util summary for Pool 0: 524288 keys, 1024 segs, 36 Mb

Type	KeyCnt	KeyUse	SegCnt	SegUse	Util	Free
0	463704	463704	909	909	99	115
1	0	0	0	0	0	115
2	0	0	0	0	0	57
3	0	0	0	0	0	29
4	0	0	0	0	0	28
Tot	463704	463704	909	909	99	115

Util summary for Pool 1: 524288 keys, 1024 segs, 36 Mb

Type	KeyCnt	KeyUse	SegCnt	SegUse	Util	Free
0	105327	105327	208	208	98	803
1	9	18	7	7	0	803
2	46	184	3	6	5	391
3	0	0	0	0	0	191
4	0	0	0	0	0	189
Tot	105382	105529	218	221	93	803

Util summary for Pool 8: 1048576 keys, 2048 segs, 72 Mb

Type	KeyCnt	KeyUse	SegCnt	SegUse	Util	Free
0	569031	569031	1117	1117	99	918
1	9	18	7	7	0	918
2	46	184	3	6	5	448
3	0	0	0	0	0	220
4	0	0	0	0	0	217
Tot	569086	569233	1127	1130	98	918

Related Commands

Command	Description
clear platform hardware cef adjacencies	Clears platform hardware CEF adjacencies.

show platform hardware cef adjacencies

To display platform hardware Cisco Express ForwardingCEF adjacencies, use the **show platform hardware cef adjacencies** command.

```

show platform hardware cef adjacencies all {detail {module {module number}}
show platform hardware cef adjacencies allocation-map {number | module {module number}}
show platform hardware cef adjacencies decap-tunnel {detail {module {module number}}}
show platform hardware cef adjacencies earl {earl-id}
show platform hardware cef adjacencies encap-tunnel {A.B.C.D | {detail {module {module number}}
show platform hardware cef adjacencies entry number | errors {module}
show platform hardware cef adjacencies mac-address {h.h.h.}
show platform hardware cef adjacencies mac-rewrite {detail | module}
show platform hardware cef adjacencies module
show platform hardware cef adjacencies mpls {detail | module}
show platform hardware cef adjacencies multicast {detail | module}
show platform hardware cef adjacencies nat {detail | module}
show platform hardware cef adjacencies recirculation {detail | module}
show platform hardware cef adjacencies resource-level
show platform hardware cef adjacencies special {module}
show platform hardware cef adjacencies status {number | module}
show platform hardware cef adjacencies tcp-intercept {detail | module}
show platform hardware cef adjacencies usage {decap-tunnel | encap-tunnel | mac-rewrite |
module | mpls | multicast | nat | recirculation | tcp-intercept}}

```

Syntax Description

all	Specifies all adjacencies.
detail	Specifies detailed information.
module	Specifies all the modules.
module number	Specifies module number.
allocation-map	Specifies the adjacency current allocation map.
allocation-map number	Specifies the starting entry. Range is 0–1048576.
decap-tunnel	Specifies the decap tunnel rewrite adjacencies.
earl earl-id	Specifies the earl-id content.

encap-tunnel	Specifies the encap tunnel rewrite adjacencies.
A.B.C.D	Specifies the IP source address.
entry number	Specifies the single adjacency entry details and the adjacency entry index. Range is 0–1048575.
errors	Specifies the adjacency application errors.
mac-address	Specifies the matched mac address adjacency.
h.h.h	Specifies the 48-bit hardware address.
mac-rewrite	Specifies the MAC rewrite adjacencies.
module module-num	Specifies the module number.
mpls	Specifies the MPLS rewrite adjacencies.
multicast	Specifies the multicast rewrite adjacencies.
nat	Specifies the NAT rewrite adjacencies.
recirculation	Specifies the recirculation rewrite adjacency.
resource-level	Specifies the adjacency watermark level and usage.
special	Specifies the special adjacencies.
status number	Shows the entries allocated or used and their owner and the starting entry. Range is 0–1048576.
tcp-intercept	Specifies the TCP-Intercept rewrite adjacency.
usage	Specifies the adjacencies usage.

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 display the CEF adjacencies allocation map module number:

```
Router# show platform hardware cef adjacencies allocation-map module 4
```

This example shows how to display the CEF adjacencies status allocated or used starting at entry 100:

```
Router# show platform hardware cef adjacencies status 100
```

```
Hardware Adjacencies used or allocated entries:
Users: "fib-ucast-v4" "fib-ucast-v6" "mpls" "vpls-ucast"
       "fib-mcast" "vpls-mcast" "acl-feature" "netflow-feat"
       "online-diag" "adjacency-mgr" "exceptions"
-----
```


Index	Owner	Status	Time
80128	netflow-feat	Allocated	*Jun 21 23:56:25.287
80129	netflow-feat	Allocated	*Jun 21 23:56:25.287
80130	netflow-feat	Allocated	*Jun 21 23:56:25.287
80131	netflow-feat	Allocated	*Jun 21 23:56:25.287
80132	netflow-feat	Allocated	*Jun 21 23:56:25.287
80133	netflow-feat	Allocated	*Jun 21 23:56:25.287
80134	netflow-feat	Allocated	*Jun 21 23:56:25.287
80135	netflow-feat	Allocated	*Jun 21 23:56:25.287
80136	netflow-feat	Allocated	*Jun 21 23:56:25.287
80137	netflow-feat	Allocated	*Jun 21 23:56:25.287
80138	netflow-feat	Allocated	*Jun 21 23:56:25.287
80139	netflow-feat	Allocated	*Jun 21 23:56:25.287
80140	netflow-feat	Allocated	*Jun 21 23:56:25.287
80141	netflow-feat	Allocated	*Jun 21 23:56:25.287
80142	netflow-feat	Allocated	*Jun 21 23:56:25.287
80143	netflow-feat	Allocated	*Jun 21 23:56:25.287
80144	netflow-feat	Allocated	*Jun 21 23:56:25.287
80145	netflow-feat	Allocated	*Jun 21 23:56:25.287
80146	netflow-feat	Allocated	*Jun 21 23:56:25.287
80147	netflow-feat	Allocated	*Jun 21 23:56:25.287
80148	netflow-feat	Allocated	*Jun 21 23:56:25.287
80149	netflow-feat	Allocated	*Jun 21 23:56:25.287
80150	netflow-feat	Allocated	*Jun 21 23:56:25.287
80151	netflow-feat	Allocated	*Jun 21 23:56:25.287
80152	netflow-feat	Allocated	*Jun 21 23:56:25.287
80153	netflow-feat	Allocated	*Jun 21 23:56:25.287
80154	netflow-feat	Allocated	*Jun 21 23:56:25.287
80155	netflow-feat	Allocated	*Jun 21 23:56:25.287
80156	netflow-feat	Allocated	*Jun 21 23:56:25.287
80157	netflow-feat	Allocated	*Jun 21 23:56:25.287
80158	netflow-feat	Allocated	*Jun 21 23:56:25.287
80159	netflow-feat	Allocated	*Jun 21 23:56:25.287
80160	netflow-feat	Allocated	*Jun 21 23:56:25.287
80161	netflow-feat	Allocated	*Jun 21 23:56:25.287
80162	netflow-feat	Allocated	*Jun 21 23:56:25.287
80163	netflow-feat	Allocated	*Jun 21 23:56:25.287
80164	netflow-feat	Allocated	*Jun 21 23:56:25.287
80165	netflow-feat	Allocated	*Jun 21 23:56:25.287
80166	netflow-feat	Allocated	*Jun 21 23:56:25.287
80167	netflow-feat	Allocated	*Jun 21 23:56:25.287
80168	netflow-feat	Allocated	*Jun 21 23:56:25.287
80169	netflow-feat	Allocated	*Jun 21 23:56:25.287
80170	netflow-feat	Allocated	*Jun 21 23:56:25.287
80171	netflow-feat	Allocated	*Jun 21 23:56:25.287
80172	netflow-feat	Allocated	*Jun 21 23:56:25.287

Router#

Related Commands**Command****Description**

**clear platform
hardware cef
adjacencies**

Clears platform hardware CEF adjacencies.

show platform hardware cef maximum-route

To display Cisco Express Forwarding (CEFv6) maximum routes, use the **show platform hardware cef maximum-routes** command in Privileged EXEC mode. This command displays both the maximum routes configuration and the current usage of entries within the dedicated area and the shared area.

show platform hardware cef maximum-routes {usage}

Syntax	Description
usage	Specifies the usage.

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 display CEFv6 maximum routes configuration and the current usage of entries within the dedicated area and the shared area:

Router# **show platform hardware cef maximum-routes**

Fib-size: 256k (262144), shared-size: 25k (25600), shared-usage: 0k(0)

Protocol	Max-routes	Use-shared-region	Dedicated
IPV4	217 k	Yes	192k
IPV4-MCAST	4 k	No	4k
IPV6	35 k	Yes	10k
IPV6-MCAST	6 k	No	6k
MPLS	5 k	No	5k
MPLS-VPN	3 k	No	3k
EoMPLS	3 k	No	3k
VPLS-IPV4-MCAST	4 k	No	4k
VPLS-IPV6-MCAST	4 k	No	4k

This example shows how to display CEFv6 accounting prefix statistics:

```
Router(config)# show platform hardware cef maximum-routes usage
Fib-size: 256k (262144), shared-size: 25k (25600), shared-usage: 0k(0)
```

Protocol	Max-routes	Usage	Usage-from-shared
-----	-----	-----	-----
IPV4	217 k	48 (0 k)	0 (0 k)
IPV4-MCAST	4 k	6 (0 k)	0 (0 k)
IPV6	35 k	2 (0 k)	0 (0 k)
IPV6-MCAST	6 k	4 (0 k)	0 (0 k)
MPLS	5 k	1 (0 k)	0 (0 k)
MPLS-VPN	3 k	0 (0 k)	0 (0 k)
EoMPLS	3 k	2 (0 k)	0 (0 k)
VPLS-IPV4-MCAST	4 k	0 (0 k)	0 (0 k)
VPLS-IPV6-MCAST	4 k	0 (0 k)	0 (0 k)

```
Router#
```

Related Commands

Command	Description
platform hardware cef maximum-route	Limits the maximum number of routes that can be programmed in the hardware.

show platform hardware database version

To display the platform hardware database version, use the **show platform hardware database** command.

show platform hardware database version [*slot slot_number*]

Syntax Description	slot <i>slot_number</i> Specifies the slot number of a module that has hardware abstraction layer (HAL) support.
---------------------------	---

Defaults	None
-----------------	------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.2(50)SY	Support for this command was introduced.
	15.0(1)SY1	The slot keyword and <i>slot_number</i> argument were added.

Usage Guidelines The **show platform hardware database** command displays the following Supervisor Engine 2T platform hardware database version:

- Bundled data
- Data from flash
- Currently used data
- Data information stored in region 1
- Data information stored in region 2
- Data information stored in golden region

The flash region has three states:

- APPROVED—The region is verified and can be used for building the hardware database.
- FIRST_RUN—The data in this region has not been verified yet, and reload is required to verify it.
- INVALID—The region is not valid.



Note It is normal for the command to display “INVALID” when the hardware database version has not been upgraded.

The **slot** keyword is supported only on modules that have hardware abstraction layer (HAL) support.

Examples

This example shows how to display the platform hardware database version:

```
Router# show platform hardware database version

Hardware database image bundle version: 2.1.0
Description: Hardware database release 2.1.0

Hardware database flash version from region S (Gold): 0.19.23

Hardware database runtime using image bundle version: 2.1.0

Region F1: INVALID
Region F2: INVALID

Region S (Golden): Version: 0.19.23
Description: change slot 7 from le_adaptive to le_gain (le_fixed)
```

Related Commands

Command	Description
upgrade hardware database	Upgrades the hardware database version.

show platform hardware earl

To display platform hardware EARL information, use the **show platform hardware earl** command.

```
show platform hardware earl {cc {table {agegrp {entry {entry number}} | bem {entry {entry number}} | bpm {entry {entry number}} | glbvlan {entry {entry number}}}} | earl_db | eureka | lamira | layer2 | wf-fpga}
```

Syntax Description

cc	Specifies the EARL consistency checker.
table	Specifies the table name.
agegrp	Specifies the Eureka age group table.
entry number	Specifies the entry in the table. Range is 0–16383.
bem	Specifies the Eureka bundle extension map table.
bpm	Specifies the Eureka bundle port map table.
glbvlan	Specifies the Eureka VLAN access mode memory.
earl_db	Specifies the EARL daughter board.
eureka	Specifies the Eureka ASIC.
lamira	Specifies the Lamira Layer 3 ASIC.
layer2	Specifies the EARL Layer2.
wf-fpga	Specifies the white field FPGA.

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 display the EARL consistency checker age group entry 4444:

```
Router(config)# show platform hardware earl cc table agegrp entry 4444
```

Related Commands

Command	Description
clear platform hardware earl	Clears platform hardware EARL information.

show platform hardware earl eureka

To display platform hardware EARL Eureka ASIC information, use the **show platform hardware earl eureka** command.

```
show platform hardware earl eureka config {all {file {word}} | module {ac {dbi | epp | ft | l2u | l2ui | l3lu | l3lu312 | l3mg | lif | lm_rx | lm_tx | ntfy | pb1_rx | pb1_tx | pb2_rx | pb2_tx | pp | rbi} | dbi | epp | ft | l2u | l2ui | l3lu | l3lu312 | l3mg | lif | lm_rx | lm_tx | ntfy | pb1_rx | pb1_tx | pb2_rx | pb2_tx | pp | rbi}}
```

```
show platform hardware earl eureka ecc {configuration {all | table {eu-acl0 | eu-acl1 | ft | lb | ldb | lifdb | lifstat | rbi}} | statistics {all | table {eu-acl0 | eu-acl1 | ft | lb | ldb | lifdb | lifstat | rbi}}}
```

```
show platform hardware earl eureka interrupts {all {file {word}} | clear {all {file} | module} | module {ac | epp | ft | l2u | l2ui | l3lu | l3lu312 | l3mg | lif | lm_rx | lm_tx | ntfy | pb1_rx | pb1_tx | pb2_rx | pb2_tx | pp | rbi | se}}
```

```
show platform hardware earl eureka statistics {all {file} | clear {all | module} | module {ac | epp | ft | l2u | l2ui | l3lu | l3lu312 | l3mg | lif | lm_rx | lm_tx | ntfy | pb1_rx | pb1_tx | pb2_rx | pb2_tx | pp | rbi | se}}
```

```
show platform hardware earl eureka vsl {mapping-tables {pb1 {dst-post-map | dst-pre-map | src-pre-map}} | pb2} | registers}
```

Syntax Description

config	Specifies the configuration register.
all	Specifies all modules.
file	Dumps the configuration registers that are not supported to a file in DFC.
word	Specifies the full name of the file. For example, disk0:/file.dat
module	Specifies modules.
ac	Specifies the AC module.
dbi	Specifies the DBI module.
epp	Specifies the epp module.
ft	Specifies the ft module.
l2u	Specifies the l2u module.
l2ui	Specifies the l2ui module.
l3lu	Specifies the l3lu module.
l3lu312	Specifies the l3lu312 module.
l3mg	Specifies the m3mg module.
lif	Specifies the LIF module.
lm_rx	Specifies the lm_rx module.
lm_tx	Specifies the lm-tx module.
ntfy	Specifies the NTFY module.
pb1_rx	Specifies the pb1_rx module.
pb1_tx	Specifies the pb1_tx module.
pb2_rx	Specifies the pb2_rx module.

pb2_tx	Specifies the pb2_tx module.
pp	Specifies the PP module.
rbi	Specifies the RBI module.
ecc	Specifies the ECC or parity error.
configuration	Specifies the ECC or parity configuration parameters.
all	Specifies all tables.
table	Specifies the memory ID.
eu_acl0	Specifies the Eureka ACL RAM 0 statistics.
eu_acl1	Specifies the Eureka ACL RAM 1 statistics.
ft	Specifies the Eureka forwarding table.
lb	Specifies the Eureka latency buffer.
ldb	Specifies the Eureka LDB port map table.
lifdb	Specifies the LIF DB.
lifstat	Specifies the LIF statistics.
rbi	Specifies the eureka RBI history FIFO.
interrupts	Specifies the interrupt statistics.
clear	Clears interrupt statistics.
statistics	Specifies the statistics.
vsl	Displays VSL configuration information.
mapping-tables	Displays VSL pre-mapping and post-mapping tables.
registers	Displays VSL control registers.
pb1	Displays PB1 mapping tables.
pb2	Displays PB2 mapping tables.
dst-post-map	Displays destination post-mapping table.
dst-pre-map	Displays destination pre-mapping table.
src-pre-map	Displays source pre-mapping table.

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 display all of EARL Eureka ASIC configurations:

```
Router# show platform hardware earl eureka config all
```

Related Commands

Command

Description

clear platform hardware earl eureka	Clears platform hardware EARL Eureka ASIC information.
--	--

show platform hardware earl lamira

To display platform hardware EARL Lamira ASIC information, use the **show platform hardware earl lamira** command.

```
show platform hardware earl lamira {config {all {file {word}}} | module {ci | cl1 | cl1_2 | cl2 |
gv | if | l3 | la0 | la1 | nf | nf2 | nf_se | pl | pl2 | po | ri | rp}} | ecc {configuration {all | table
{acct | aclsram-a | aclsram-b | acltcam-a | acltcam-b | acosseli | adj-dram | adjstats | agdpp
| cmtbla | cmtblb | dagram | egmtmap | elifmap | fib-dram | fibtcam | ife_dstinfo | iferdtd |
ilifmap | infife | infofe | label2sela | label2selb | lcbent | nffl | nfflhash0 | nfflhash1 | nfflstats |
nffltable | nfflvram | ofe_dstinfo | ofeff | oferdtd | outff | plcbas | pmap | rit | rpfdrum | rwsel |
sagram | smpl | srcdstas | vidmap | vlanmap}}} | statistics {all | table {acct | aclsram-a |
aclsram-b | acltcam-a | acltcam-b | acosseli | adj-dram | adjstats | agdpp | cmtbla | cmtblb |
dagram | egmtmap | elifmap | fib-dram | fibtcam | ife_dstinfo | iferdtd | ilifmap | infife |
infofe | label2sela | label2selb | lcbent | nffl | nfflhash0 | nfflhash1 | nfflstats | nffltable | nfflvram |
ofe_dstinfo | ofeff | oferdtd | outff | plcbas | pmap | rit | rpfdrum | rwsel | sagram | smpl |
srcdstas | vidmap | vlanmap}}} | interrupts {all {file {word}} | clear {all {file} | module
{cl1 | cl1_2 | cl2 | gv | if | l3 | la0 | la1 | nf | nf2 | nf_se | pl | pl2 | po | ri | rp}} | module} |
statistics {all {file {word}} | clear {all | module {ci | cl1 | cl1_2 | cl2 | gv | if | l3 | la0 | la1 |
nf | nf2 | nf_se | pl | pl2 | po | ri | rp}} | module}}
```

Syntax Description

config	Specifies the configuration register.
all	Displays all modules.
file	Dumps the configuration registers to a file that are not supported in DFC.
word	Specifies the full name of the file.
module	Specifies modules.
ci	Specifies the module CI.
cl1	Specifies the module CL1.
cl1_2	Specifies the module CL1_2.
cl2	Specifies the module CL2.
gv	Specifies the module GV.
if	Specifies the module IF.
l3	Specifies the module L3.
la0	Specifies the module LA0.
la1	Specifies the module LA1.
nf	Specifies the module NF.
nf2	Specifies the module NF2.
nf_se	Specifies the module NF_SE.
pl	Specifies the module PL.
pl2	Specifies the module PL2.
po	Specifies the module PO.
ri	Specifies the module RI.
rp	Specifies the module RP.
ecc	Specifies the ECC or parity error.
configuration	Specifies the ECC or parity configuration parameters.

all	Specifies all tables.
table	Specifies the memory ID.
statistics	Specifies the ECC or parity error statistics.
table	Displays the memory ID.
acct	Specifies the Lamira ACCT_STATS_MEM.
aclsram-a	Specifies the Lamira ACL_SRAM_A.
aclsram-b	Specifies the Lamira ACL_SRAM_B.
acltcam-a	Specifies the Lamira ACL_TCAM_A.
acltcam-b	Specifies the Lamira ACL_TCAM_B.
acosseli	Specifies the Lamira ACOS_SEL_CTRL_TBL.
adj-dram	Specifies the Lamira ADJ_DRAM.
adjstats	Specifies the Lamira ADJ_STATS.
agdpp	Specifies the Lamira AG_DPP_TBL.
cmtbla	Specifies the Lamira CM TBL A.
cmtblb	Specifies the Lamira CM TBL B.
dagram	Specifies the Lamira D_AGRAM.
egmtmap	Specifies the Lamira EG_MT_MAP.
elifmap	Specifies the Lamira EGRESS_LIF_MAP.
fib-dram	Specifies the Lamira FIB_DRAM.
fibtcam	Specifies the Lamira FIB_TCAM.
ife_dstinfo	Specifies the Lamira IFE_DST_INFO_TBL.
iferdt	Specifies the Lamira IFE_RDT_TBL.
ilifmap	Specifies the Lamira INGRESS_LIF_MAP.
infife	Specifies the Lamira INF_FF_IFE.
infofe	Specifies the Lamira INF_FF_OFE.
label2sela	Specifies the Lamira LABEL2SEL_A.
label2selb	Specifies the Lamira LABEL2SEL_B.
lcbcnt	Specifies the Lamira LC_BCNT_TBL.
nffl	Specifies the Lamira NF_FL_TABLE.
nfhash0	Specifies the Lamira NF_HASH_0.
nfhash1	Specifies the Lamira NF_HASH_1.
nfstats	Specifies the Lamira NF_STATS.
nftable	Specifies the Lamira NF_TABLE.
nfvrsm	Specifies the Lamira NF_VRAM.
ofe_dstinfo	Specifies the Lamira OFE_DST_INFO_TBL.
ofeff	Specifies the Lamira OFE_FF.
oferdt	Specifies the Lamira OFE_RDT_TBL.
outff	Specifies the Lamira OUT_FF.
plcbas	Specifies the Lamira PLC_BAS_XLT_TBL.
pmap	Specifies the Lamira PMAP.
rit	Specifies the Lamira RIT.

rpf dram	Specifies the Lamira RPF_DRAM.
r wsel	Specifies the Lamira RW_SEL.
s agram	Specifies the Lamira S_AGRAM.
smpl	Specifies the Lamira SMPL_TBL.
srcdstas L	Specifies the Lamira SRC_DST_AS_TB.
vidmap	Specifies the Lamira VID MAP.
vlanmap	Specifies the Lamira VLAN MAP.
interrupts	Specifies interrupts 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 display all of the EARL Lamira ASIC configuration:

```
Router# show platform hardware earl lamira config all
```

Related Commands

Command	Description
clear platform hardware earl lamira	Clears platform hardware EARL Lamira ASIC information.

show platform hardware earl layer2

To display platform hardware EARL Layer 2 information, use the **show platform hardware earl layer2** command.

```
show platform hardware earl layer2 {etherchannel {bem-table {number number} | bpm-table
{bridge-domain number} | config} | forwarding-table {dump {all | l2addr number} | l2addr
{H.H.H}} | redirections {protocol-filtering {dump {all | dot1ad | dot1q | vpls} |
profile-map}}}
```

Syntax Description		
etherchannel		Specifies the Layer 2 and Layer 3 EtherChannel forwarding-related parameters.
bem-table number	<i>number</i>	Specifies the Bundle Expansion Map table number. Range is 0–7.
bpm-table		Specifies the Bundle Port Map table.
bridge-domain number	<i>number</i>	Specifies the bridge domain number. Range is 0–16383.
config		Specifies all the EtherChannel-related hardware configuration.
forwarding-table		Specifies the Layer 2 forwarding table-related parameters.
dump		Specifies the valid entries to dump.
all		Specifies that all the entries need to be dumped.
l2addr number	<i>number</i>	Specifies the number of Layer 2 addresses that need to be dumped. Range is 0–131071.
l2addr		Specifies the computation of the Layer 2 table address.
H.H.H		Specifies the 48-bit MAC address.
redirections		Specifies the Layer 2, Layer 3, and Layer 4 redirections-related parameters.
protocol-filtering		Specifies the protocol filtering-related parameters.
dot1ad		Specifies that dot1ad profile needs to be dumped.
dot1q		Specifies that dot1q profile needs to be dumped.
vpls		Specifies that VPLS profile needs to be dumped.
profile-map		Specifies that the logical-to-physical (hardware) mapping of profiles needs to be printed.

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 display platform hardware EARL Layer 2 EtherChannel BPM table, bridge domain 4:

```
Router# show platform hardware earl layer2 etherchannel bpm-table bridge-domain 4
```

Related Commands

Command	Description
platform hardware earl layer2	Configures the platform hardware EARL for Layer 2.

show platform hardware efp

To display hardware EFP configuration, use the **show platform hardware efp** command.

```
show platform hardware efp { config { gigabitethernet number | port-channel number |
tengigabitethernet number } | datapath { gigabitethernet number | port-channel number |
tengigabitethernet number } | global }
```

Syntax Description	Parameter	Description
	config	Specifies the EFP configuration information.
	gigabitethernet <i>number</i>	Specifies the Gigabit Ethernet by number.
	port-channel <i>number</i>	Specifies the Ethernet channel of interfaces by number. Range is 1–496.
	tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet by number.
	datapath	Specifies the EFP datapath information.
	global	Specifies the EFP global 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 display the hardware EFP configuration information for Gigabit Ethernet 4:

```
Router# show platform hardware efp config gigabitethernet 4
```

Related Commands	Command	Description
	platform hardware efp	Configures the platform hardware EFP.

show platform hardware fan-tray

To display hardware fan tray status or details by number, use the **show platform hardware fan-tray** command.

show platform hardware fan-tray {*number* | **status**}

Syntax Description	
<i>number</i>	Specifies the fan tray number. Range is 1–1.
status	Specifies the fan tray status.

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 display the hardware details for fan tray 1: Router# show platform hardware fan-tray 1
----------	--

Related Commands	Command	Description
	platform hardware fan-tray	Configures the platform hardware fan tray.

show platform hardware flow table

To display hardware flow table entries, use the **show platform hardware flow table** command.

```
show platform hardware flow table {copy-policy index | flowmask {index | ip index | ipv6 index | l2 index | mpls index} | mark-en-map index | profile {index | ip index | ipv6 index | l2 index | mpls index} | qos-ctrl index | redirect {ife index | ofe index | tcp index} | sampler index | sampler-copy index | shadow {copy-policy index | flowmask {index | ip index | ipv6 index | l2 index | mpls index} | mark-en-map index | profile {index | ip index | ipv6 index | l2 index | mpls index} | qos-ctrl index | redirect {ife index | ofe index | tcp index} | sampler index | sampler-copy index}}
```

Syntax Description		
copy-policy <i>index</i>		Specifies the copy policy entries by index number. Range is 0–31.
flowmask <i>index</i>		Specifies the flow mask entries by index number. Range is 0–79.
ip <i>index</i>		Specifies the IP entries by index number. Range is 0–31.
ipv6 <i>index</i>		Specifies the IPv6 entries by index number. Range is 0–31.
l2 <i>index</i>		Specifies the Layer 2 entries by index number. Range is 0–7.
mpls <i>index</i>		Specifies the MPLS entries by index number. Range is 0–7.
mark-en-map <i>index</i>		Specifies the mark encapsulation map entries by index number. Range is 0–63.
profile <i>index</i>		Specifies the profile entries by index number. Range is 0–79.
qos-ctrl <i>index</i>		Specifies the QoS CTRL entries by index number. Range is 0–63.
redirect		Specifies the redirect tables.
ife <i>index</i>		Specifies the IFE redirect by index number. Range is 0–511.
ofe <i>index</i>		Specifies the OFE redirect by index number. Range is 0–511.
tcp <i>index</i>		Specifies the TCP redirect by index number. Range is 0–7.
sampler <i>index</i>		Specifies the sampler entry by index number. Range is 0–1023.
sampler-copy <i>index</i>		Specifies the sampler copy entry by index number. Range is 0–7.
shadow		Specifies the shadow extension tables.

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 display the hardware flow table entries for IFE redirect index 4:

```
Router# show platform hardware flow table redirect ife 4
```

Related Commands

Command	Description
platform hardware flow table	Configures the platform hardware flow table entries.

show platform hardware fpoe

To display hardware Fabric Port of Exit (FPoE) by slot number, use the **show platform hardware fpoe** command.

```
show platform hardware fpoe {slot number}
```

Syntax Description	<i>slot number</i>	Specifies the module number.
---------------------------	--------------------	------------------------------

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 display the hardware FPoE for slot 4: Router# show platform hardware fpoe slot 4
-----------------	--

Related Commands	Command	Description
	platform hardware fpoe	Configures platform hardware FPoE by slot number.

show platform hardware idprom

To display information on EEPROM for the platform hardware, use the **show platform hardware idprom** command.

```
show platform hardware idprom {backplane number | clock number | earl number |
fabric-extension number | fan-tray number | module number | power-supply number | rp
number | supervisor number | vdb number | vtt number}
```

Syntax Description

backplane number	Displays the backplane EEPROM number. Range is 1–2.
clock number	Specifies the clock EEPROM number. Range is 1–2.
earl number	Specifies the EARL EEPROM number.
fabric-extension number	Specifies the fabric extension board's EEPROM number.
fan-tray number	Specifies the fan tray EEPROM number. Range is 1–1.
module number	Specifies the module EEPROM number.
power-supply number	Specifies the power supply EEPROM number. Range is 1–2.
rp number	Specifies the RP EEPROM.
supervisor number	Specifies the supervisor EEPROM.
vdb number	Specifies the VDB EEPROM number.
vtt number	Specifies the VTT EEPROM number. Range is 1–4.

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 display the information on the EEPROM for backplane 1:

```
Router# show platform hardware idprom backplane 1
```

Related Commands

Command	Description
platform hardware idprom	Configures the information on the EEPROM for the platform hardware.

show platform hardware image version slot

To display the hardware abstraction layer (HAL) image version information, use the **show platform hardware image version** command.

show platform hardware image version slot *number*

Syntax Description	slot <i>number</i>	Specifies the module slot number.
---------------------------	---------------------------	-----------------------------------

Defaults	None	
-----------------	------	--

Command Modes	Privileged EXEC mode	
----------------------	----------------------	--

Command History	Release	Modification
	15.0(1)SY1	Support for this command was introduced.

Usage Guidelines	This command is useful only if a new hardware image version becomes available. This command is supported only on modules that have hardware abstraction layer (HAL) support.
-------------------------	---

Examples This example shows how to display the HAL image version information for a module:

```
Router# show platform hardware image version slot 3
Image bundle version: 1.1

Linecard image version from region S(Golden): INVALID

Image runtime using image bundle version: 1.1

Region F1: INVALID, version: INVALID
Region S (Golden): version: INVALID
```



Note It is normal for the command to display “INVALID” when the version has not been upgraded.

Related Commands	Command	Description
		upgrade hardware image

show platform hardware lif l2

To display platform hardware Layer 2 LIF information, use the **show platform hardware lif l2** command.

```
show platform hardware lif l2 {globalcfg | memory {memory detail} | region {adjacency {dti
{adjacency number | config} | replicated {adjacency | config}} | egresslif {config | lif {lif
number}} | flood {config | ltl} | globalvlan {config | vlan} | negative-mn {config | ltl} |
portgroup {config | ltl} | shim {config | lif} | swltl {config | ltl} | vb {config | vlan}} | table
{global-vlan vlan | lif-db {all | entry number | key} | port-map {all | interface
{gigabitethernet | longreachethernet | multilink | port-channel | tengigabitethernet} |
ltl-index number}}}
```

Syntax Description

globalcfg	Specifies the global configuration.
memory	Specifies the free memory.
memory detail	Specifies the detailed memory list.
region	Specifies the region.
adjacency	Specifies the adjacency region.
dti	Specifies the DTI.
adjacency number	Specifies the valid adjacency. Range is 0–2047999.
config	Specifies the configuration.
replicated	Specifies the replication.
egresslif	Specifies the egress LIF region.
lif	Specifies the LIF keyword.
lif number	Specifies the valid LIF number. Range is 0–131071.
flood	Specifies the flood region.
ltl	Specifies the LTL index.
globalvlan vlan	Specifies the global VLAN region.
vlan	Specifies the VLAN keyword.
negative-mn	Specifies the negative MN region.
portgroup	Specifies the port group region.
shim	Specifies the SHIM/ SVC LIF region.
swltl	Specifies the SW LTL region.
vb	Specifies the VB region.
table	Specifies the Layer 2 LIF tables.
global-vlan	Specifies the global VLAN table.
lif-db	Specifies the LIF database.
all	Specifies that all uninitialized values need to be printed.
entry number	Specifies the LIF database entry, and the valid LIF database address. Range is 0–262143.
key	Specifies the LIF database table key.
port-map	Specifies the port map.
interface	Specifies the interface.

gigabitethernet	Specifies the Gigabit Ethernet IEEE 802.3z.
longreachethernet	Specifies the long-reach Ethernet interface.
multilink	Specifies the multilink group interface.
port-channel	Specifies the Ethernet channel interface.
tengigabitethernet	Specifies the 10-Gigabit Ethernet.
ltl-index <i>number</i>	Specifies the valid LTL index. Range is 0–16383.

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 display platform hardware Layer 2 LIF global configuration:

```
Router# show platform hardware lif 12 globalcfg
```

Related Commands	Command	Description
	platform hardware lif 12	Configures the platform hardware LIF for Layer 2.

show platform hardware lif l3

To display platform hardware Layer 3 LIF information, use the **show platform hardware lif l3** command.

```
show platform hardware lif l3 {egress {features | handle | hierarchy | index | interface | ipv4 |
  ipv6 | misc | module | mpls | qos} | info number | ingress { features | handle | hierarchy |
  index | interface | ipv4 | ipv6 | misc | module | mpls | qos} | mtu { table {dump | index}} |
  port-map{ index number | interface {gigabitethernet | port-channel | tengigabitethernet
  tunnel | vlan} | module number}}
```

Syntax Description

egress	Specifies the egress entry information.
features	Displays the features-related fields.
handle	Specifies the LIF entry handle.
hierarchy	Displays the entry with inheritance hierarchy.
index	Specifies the LIF entry index.
interface	Specifies the interface name.
ipv4	Displays IPv4-related fields.
ipv6	Displays IPv6-related fields.
misc	Displays the miscellaneous fields.
module	Specifies the selected module for the command.
mpls	Displays the MPLS-related fields.
qos	Displays the QoS-related fields.
info <i>number</i>	Displays the LIF table-related information and specifies the LIF test number. Range is 0–4294967295.
ingress	Specifies the ingress entry information.
mtu	Specifies the MTU information.
table	Specifies the hardware MTU table information.
dump	Specifies the Layer 3 hardware LIF table that needs to be dumped.
index <i>number</i>	Specifies the hardware MTU table information.
port-map	Specifies the port map entry information.
index	Specifies the Layer 3 port map entry index.
gigabitethernet	Specifies the Gigabit Ethernet IEEE 802.3z.
port-channel	Specifies the Ethernet channel interface.
tengigabitethernet	Specifies the 10-Gigabit Ethernet.
tunnel	Specifies the tunnel interface.
vlan	Specifies the VLANs.
module <i>number</i>	Specifies the selected module for the command.

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 display platform hardware EARL Layer 3 LIF test number 4:

```
Router# show platform hardware lif 13 info 4
```

Related Commands	Command	Description
	platform hardware lif 13	Configures the platform hardware LIF for Layer 3.

show platform hardware lif stats

To display hardware LIF statistics, use the **show platform hardware lif stats** command.

```
show platform hardware lif stats {index number | interface {gigabitethernet | port-channel |
tengigabitethernet | tunnel | vlan} | profile {choice {all {module} | id number} |
read{module} | write number} | table {config {module} | egress {module} | fop {module} |
ingress {module} | no-stat {module} | status {module}}}
```

Syntax Description

index <i>number</i>	Specifies the LIF statistics for a particular index. Range is 0–131071.
interface	Specifies the interface name.
gigabitethernet	Specifies the Gigabit Ethernet IEEE 802.3z.
port-channel	Specifies the Ethernet channel interface.
tengigabitethernet	Specifies the 10-Gigabit Ethernet.
tunnel	Specifies the tunnel interface.
vlan	Specifies the VLANs.
profile	Specifies the LIF statistic profile information.
choice	Specifies the choice of LIF statistics profiles.
all	Specifies that the summary of all the available LIF statistics profiles need to be printed.
module	Specifies the module selected for the command.
id <i>number</i>	Specifies that the details of the matching LIF statistics profile ID need to be printed. Range is 0–6.
read	Specifies that the current LIF statistics profile needs to be printed.
write <i>number</i>	Sets the LIF statistics profile according to the given valid profile index. Range is 0–6.
table	Specifies the LIF statistics input tables.
config	Specifies that the LIF statistics config register values needs to be printed.
egress	Specifies that the egress LIF statistics input table needs to be printed.
fop	Specifies that the forwarding operation memory table needs to be printed.
ingress	Specifies that the ingress LIF statistics input table needs to be printed.
no-stat	Specifies that the LIF no-statistics register values need to be printed.
status	Specifies that the status of the LIF statistics register values need to be printed.

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 display platform hardware LIF statistics for index 4:

```
Router# show platform hardware lif stats index 4
```

Related Commands

Command	Description
platform hardware lif stats	Configures the platform hardware LIF statistics.

show platform hardware ltl

To display information on LTL for the platform hardware, use the **show platform hardware ltl** command.

```
show platform hardware ltl { index number | interface { gigabitethernet number | tengigabitethernet number } | slot number | vlan vlan_id }
```

Syntax Description

index <i>number</i>	Displays the LTL hardware setting on an index. Range is 0–65535.
interface	Specifies the type of interface.
gigabitethernet <i>number</i>	Specifies the Gigabit Ethernet number.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet number.
slot <i>number</i>	Specifies the slot number.
vlan <i>vlan_id</i>	Specifies the VLAN number. Range is 0–4096.

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 display the LTL information for Gigabit Ethernet 4:

```
Router# show platform hardware ltl interface gigabitethernet 4
```

Related Commands

Command	Description
platform hardware ltl	Configures the LTL information.

show platform hardware multicast routing

To match and display multicast routing entries in hardware for multicast IPv4 and IPv6 addresses, use the **show platform hardware multicast routing** command in privileged EXEC mode.

```
show platform hardware multicast routing {ip | ipv6} group {ip-addr [detail | verbose]}
```

Syntax Description	ip	Shows the hardware entries for IPv4.
	ipv6	Shows the hardware entries for IPv6.
	group	Shows the hardware entries for a group.
	ip-addr detail	Shows the hardware entry details.
	ip-addr verbose	Shows the hardware entry verbose details.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines The **show platform hardware multicast routing ip group** command displays multicast OIFs.

Examples This example shows how to display the hardware detail entries:

```
Router# show platform hardware multicast routing ip group 226.1.1.1 detail
(10.1.1.1, 226.1.1.1/32)
  FIBAddr: 0xB00 IOSVPN: 0 RpfType: SglRpfChk SrcRpf: Gi1/1
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAAdjPtr: 0x30002 Format: IP rdt: off elif: 0xC5408
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: on mtu_idx: 2(1518)
  PV: 1 rwtype: MCAST_L3_RWT_L2_EXPS
  met3: 0x19 met2: 0x18
  Packets: 0          Bytes: 0

  NPIAdjPtr: 0x30003 Format: IP rdt: on elif: 0xC5408
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off
  PV: 0 rwtype: MCAST_L3_REWRITE
  met3: 0x20 met2: 0x0 DestNdx: 0x7FF3

  Packets: 0          Bytes: 0
  MET offset: 0x19
    OIF          AdjPtr          Elif          CR
  +-----+-----+-----+-----+
    EDT-50001    0x50001    0x8400A    1T1 5T1/T2
  MET offset: 0x20
```

```

          OIF          AdjPtr      Elif          CR
+-----+-----+-----+-----+
  Gi1/2          0xA8000      0xA4012      1T1
MET offset: 0x18
          LBL          IF          AdjPtr      Elif          CR
+-----+-----+-----+-----+
  20              Gi3/9          0xA8000      0xA4013      3T1/T2
Router#

```

This example shows how to display the hardware verbose entries:

```

Router# show platform hardware multicast routing ip group 226.1.1.1 verbose
(10.0.0.2, 226.1.1.1/32)
  FIBAddr: 0x2A04 IOSVPN: 0 RpfType: SglRpfChk SrcRpf: Po1
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAAdjPtr: 0x30003 Format: IP rdt: off elif: 0xC5408
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: on mtu_idx: 2(1518)
  PV: 1 rwtype: MCAST_L3_RWT_L2_EXPS
  met3: 0x18 met2: 0x18
  Packets: 31912689      Bytes: 15956344500

  NPIAdjPtr: 0x30004 Format: IP rdt: on elif: 0xC5408
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off
  PV: 0 rwtype: MCAST_L3_REWRITE
  met3: 0x5 met2: 0x0 DestNdx: 0x7FF3
  Packets: 1263         Bytes: 631500

  OIF: V19 OIFAdjPtr: 0x8009 Format: IP rdt: off elif: 0x9
  fltr_en: on idx_sel/bndl_en: 1 dec_ttl: off
  PV: 0 rwtype: L3_REWRITE
  smac_rwt: 1 smac: 000e.39c2.b540 ip_to_mac: 1

  OIF: EDT-50001 OIFAdjPtr: 0x50001 Format: MDT rdt: on elif: 0x8400A
  fltr_en: off idx_sel/bndl_en: 1 dec_ttl: off
  PV: 0 rwtype: L3_REWRITE add_shim: 1
  rec_shim_op: DTI_FROM_RIT rec_dti_type: RSVD3 rec_data: 0x701A0000 eg_mcast_dist: 1
  DestNdx: 0x80D RBH: 0x0
  DestNdx: 0x80D RBH: 0x1
  DestNdx: 0x80D RBH: 0x2
  DestNdx: 0x80D RBH: 0x3
  DestNdx: 0x80D RBH: 0x4
  DestNdx: 0x80D RBH: 0x5
  DestNdx: 0x80D RBH: 0x6
  DestNdx: 0x80D RBH: 0x7

  LBL: 20 OIFAdjPtr: 0xA8000 Format: MPLS rdt: on elif: 0xA4013
  LBL_OP: push dec_ttl: on
  PV: 0 rwtype: L3_REWRITE
  smac_rwt: 1 smac: 000e.39c2.b540 dmac_rwt: 1 dmac: 000e.39c2a123
Router#

```

Related Commands

Command	Description
debug platform software multicast routing	Displays information about multicast errors.
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.

Command	Description
show platform hardware cef mpls detail	Displays MPLS CEF detail information.
show platform hardware met read	Displays platform hardware MET table entries.
show platform software met detail	Displays software routing for the MET.

show platform hardware met read

To display platform hardware MET table entries, use the **show platform hardware met read** command in privileged EXEC mode.

```
show platform hardware met read {slot slot-num | port port-num {addr addr}}
```

Syntax Description

slot <i>slot-num</i>	Displays the hardware MET table for the corresponding slot.
port <i>port-num</i>	Displays the hardware MET entries for a port.
addr <i>addr</i>	Displays the hardware MET information for the address of the slot or port.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

The **show platform hardware met read** command displays MET table entry information. For each adjacency use the **show platform hardware cef adjacencies entry** command to display the MPLS adjacency information.

Examples

This example shows how to display the hardware MET table entries for slot 1 address 18:

```
Router# show platform hardware met read slot 1 addr 18
  Starting Offset: 0x0018
  V E C:3989 I:0x00000 (A: 0x0A8000)
Router#
```

Related Commands

Command	Description
debug platform software multicast routing	Displays information about multicast errors.
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 software met detail	Displays software routing for the MET.

show platform hardware statistics

To display platform hardware statistics, use the **show platform hardware statistics** command.

show platform hardware statistics {**drop** | **exception** | **module** *number*}

Syntax Description	drop	Displays the dropped statistics.
	exception	Displays the statistics that have an exception.
	module <i>number</i>	Specifies the module number.

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 display platform hardware statistics for module 4:

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

Related Commands	Command	Description
	clear platform hardware statistics	Clears the statistics.

show platform hardware transceiver xml version

To display the hardware abstraction layer (HAL) transceiver XML version information, use the **show platform hardware transceiver xml version** command.

show platform hardware transceiver xml version

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Privileged EXEC mode

Command History	Release	Modification
	15.0(1)SY1	Support for this command was introduced.

Usage Guidelines This command is useful only if a new transceiver XML version becomes available.

Examples This example shows how to display the HAL transceiver XML version information:

```
Router# show platform hardware transceiver xml version
Transceiver image bundle version: INVALID
Transceiver disk version : INVALID
Transceiver runtime using image bundle version: INVALID

region F1: INVALID
region F2: INVALID
```



Note

It is normal for the command to display “INVALID” when the transceiver XML version has not been upgraded.

Related Commands	Command	Description
	upgrade hardware transceiver xml	Upgrades the XML version.

show platform hardware virtual-map

To display virtual map information, use the **show platform hardware virtual-map** command.

show platform hardware virtual-map

Syntax Description This command has no arguments or keywords.

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 display virtual map information:

```
Router# show platform hardware virtual-map
```

Related Commands	Command	Description
	platform hardware virtual-map	Configures the virtual map.

show platform hardware xml version

To display the hardware abstraction layer (HAL) XML version information, use the **show platform hardware xml version** command.

```
show platform hardware xml version {slot number | file name}
```

Syntax Description

slot number	Specifies the module slot number.
file name	Specifies an XML file name.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.0(1)SY1	Support for this command was introduced.

Usage Guidelines

This command is useful only if a new XML version becomes available.

This command is supported only on modules that have hardware abstraction layer (HAL) support.

Examples

This example shows how to display the HAL XML version information for a module:

```
Router# show platform hardware xml version slot 4
XML image bundle version: 1.1

Linecard XML version from region S(Golden): INVALID

XML runtime using image bundle version: 1.1

Region F1: INVALID, version: INVALID
Region F2: INVALID, version: INVALID
Region S (Golden): version: INVALID
```



Note

It is normal for the command to display “INVALID” when the XML version has not been upgraded.

Related Commands

Command	Description
upgrade hardware xml	Upgrades the XML version.

show platform idbhal

To display information about platform interface detector block (IDB) management, use the **show platform idbhal** command.

```
show platform idbhal {applications detail | conversion {fib {lif number | ltl-index number | mih number} | lif number | mih number} | interface {gigabitethernet number | null | port-channel number | tengigabitethernet number | tunnel number | vlan vlan_id | detail} | process}
```

Syntax Description

applications <i>detail</i>	Displays application-related information in detail.
conversion	Displays conversion database-related information.
fib	Displays FIB conversion database information.
lif <i>number</i>	Specifies the LIF number. Range is 0–1F3FF.
ltl-index <i>number</i>	Specifies the LTL index number. Range is 0–7FF.
mih <i>number</i>	Specifies the MIH number. Range is 0–FFFFFFFE.
interface	Displays interface-related information.
gigabitethernet <i>number</i>	Specifies the GigabitEthernet interface number.
null	Specifies the null interface.
port-channel <i>number</i>	Specifies the Ethernet channel of interfaces number. Range is 1–496.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 0–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN number. Range is 1–4094.
detail	Displays detailed interface information.
process	Displays process-related information.

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 display information for IDB interface tengigabitethernet 4:

```
Router# show platform idbhal interface tengigabitethernet 4
```

Related Commands

Command	Description
platform idbhal	Configures platform IDB management.

show platform idbhal conversion

To view platform IDBHAL conversion information, use the **show platform idbhal conversion** command.

```
show platform idbhal conversion { fib { lif number | ltl-index number | mih number } | lif number | mih number }
```

Syntax Description	Parameter	Description
	fib	Specifies the FIB conversion database.
	<i>lif number</i>	Specifies the LIF number in LIF to IDB conversion database. Range: 0–1F3FF.
	ltl-index number	Specifies the LTL index number in LTL index to FIBIDB conversion database. Range: 0–7FF.
	<i>mih number</i>	Specifies the MIH number in MIH to IDB conversion database. Range: 0–FFFFFFFE.

Defaults There are no defaults for this command.

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 view platform hardware IDBHAL conversion for LIF 4:

```
Router# show platform idbhal conversion lif 4
```

Related Commands	Command	Description
	platform idbhal conversion	Configures the platform IDBHAL conversion process.

show platform ip rsvp

To display RSVP information for the platform IP, use the **show platform ip rsvp** command.

```
show platform ip rsvp {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 | fcpa number | statistics
| voabypassin number | voabypassout number | voafilterin number | voafilterout number |
voain number | voaout number}} | netflow identity-string | statistics identity-string }
```

Syntax Description

interface	Displays the RSVP information for a particular interface.
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.
filter number	Specifies the filter interface number.
filtergroup number	Specifies the filter group interface number.
gigabitethernet number	Specifies the gigabit ethernet interface number.
longreachethernet number	Specifies the long-reach Ethernet interface number.
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.
pos-channel number	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock number	Specifies the telecom-bus Clock Controller interface number.
tengigabitethernet number	Specifies the 10-Gigabit Ethernet interface number.
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 <i>number</i>	Specifies the fibre channel interface number.
control-plane <i>number</i>	Specifies the control plane interface number.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number.
voain <i>number</i>	Specifies the VOA in interface number.
voaout <i>number</i>	Specifies the VOA out interface number.
netflow <i>identity-string</i>	Displays information related to NetFlow.
statistics <i>identity-string</i>	Displays statistics information related to NetFlow.

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 display the RSVP information for the platform IP with asynchronous interface 4:

```
Router# show platform ip rsvp interface async 4
```

Related Commands	Command	Description
	platform ip rsvp	Configures the platform IP RSVP keyword.

show platform l2transport gre

To display platform details of Layer 2 over generic routing encapsulation (GRE) tunnel, use the **show platform l2transport gre** command.

```
show platform l2transport gre { nodes | summary tunnel _if _number | vlan vlan_id <peerrid>
clear-counter }
```

Syntax Description	Parameter	Description
	nodes	Specifies Layer 2 GRE nodes.
	summary	Specifies Layer 2 GRE summary information.
	<i>tunnel _if _number</i>	Specifies tunnel information by number. Range is 1–4294967295.
	vlan vlan_id	Specifies VLAN information. Range is 1–4092.
	<i>peerid</i> or <i>peerip</i>	Specifies the virtual connection information between the local node and remote peer, and the traffic statistics.
	<i>clear-counter</i>	Clears the traffic statistics for the virtual connection; note the counters are updated every 10 seconds, sometimes you need to wait for 10 seconds for the updated counters.

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 display platform details of Layer 2 over GRE tunnel 4:

```
Router# show platform l2transport gre tunnel 4
```

Related Commands	Command	Description
	platform l2transport gre	Configures the platform details of Layer 2 over GRE tunnel.

show platform mrm info

To display platform Match Register Manager (MRM) usage, use the **show platform mrm info** command.

show platform mrm info

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 display platform MRM usage:

```
Router# show platform mrm info
```

Related Commands	Command	Description
	platform mrm info	Configures the platform Match Register Manager (MRM) usage.

show platform multicast routing

To display multicast configuration in routing mode, use the **show platform multicast routing** command.

show platform multicast routing { replication }

Syntax Description	replication	Specifies replication mode configuration.
---------------------------	--------------------	---

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	<p>This example shows how to display LTL-sharing across VLANs in multicast routing configuration:</p> <pre>Router# show platform multicast routing replication</pre>	
-----------------	--	--

Related Commands	Command	Description
	platform multicast routing	Configures the multicast routing information for the platform.

show platform nvhmr

To display platform Non-Volatile Health Monitor Record (NVHMR), use the **show platform nvhmr** command.

```
show platform nvhmr { current { all | entry number | summary } | previous { all | entry number | summary } }
```

Syntax Description	current	Specifies NVHMR for the current running instance.
	all	Displays all information on specified NVHMR.
	entry number	Displays information on specified NVHMR for entry number. Range is 0–5.
	summary	Displays summary information for specified NVHMR.
	previous	Specifies NVHMR for the previously ran instance.

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 display platform NVHMR of current entry number 4: Router# show platform nvhmr current entry 4
----------	---

Related Commands	Command	Description
	platform nvhmr	Configures the platform NVHMR.

show platform qos aggregate policer

To display information about the aggregate policer for platform quality of service (QoS), use the **show platform qos aggregate policer** command in EXEC mode.

```
show platform qos aggregate policer [aggregate-name]
```

Syntax Description	<i>aggregate-name</i> (Optional) Name of the aggregate policer.				
Command Default	None				
Command Modes	EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(50)SY</td> <td>Support for this command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(50)SY	Support for this command was introduced.
Release	Modification				
12.2(50)SY	Support for this command was introduced.				

Usage Guidelines

Aggregate policing works independently on each Distributed Forwarding Card (DFC)-equipped switching module and independently on the Policy Feature Card 2 (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, the PFC2, and any non-DFC-equipped switching modules that are supported by the PFC2.

Examples

This example shows how to display information about the aggregate policer for platform QoS:

```
Router# show platform qos aggregate-policer

ag1 (undefined)
  AgId=0 [ pol1 pol2 ]
ag2 64000 64000 conform-action set-dscp-transmit 56 exceed-action drop
  AgId=0 [ pol3 ]
ag3 32000 32000 conform-action set-dscp-transmit 34 exceed-action drop
```

In the output, the following applies:

- The **AgId** parameter displays the hardware-policer ID and is nonzero if assigned.
- The policy maps using the policer, if any, are listed in the square brackets ([]).
- If there are no policies using the policer, no **AgId** line is displayed.
- If the policer is referred to in policy maps, but has not been defined, [**undefined**] is displayed.

Related Commands

Command	Description
platform qos aggregate-policer	Defines a named aggregate policer for use in policy maps.

show platform qos maps

To display platform quality of service (QoS) mapping information, use the **show platform qos maps** command in privileged EXEC mode.

Cisco 2600, 3660, 3700, 3845, 7200, 7400, and 7500 Series Routers

```
show platform qos maps [cos-dscp | dscp-cos]
```

Cisco 7600 Series Router and Catalyst 6500 Series Switch

```
show platform qos maps [cos-dscp | cos-mutation | dscp-cos | dscp-exp | dscp-mutation |
exp-dscp | exp-mutation | ip-prec-dscp | policed-dscp]
```

Syntax	Description
cos-dscp	(Optional) Displays the class of service (CoS)-to-differentiated services code point (DSCP) map.
dscp-cos	(Optional) Displays the DSCP-to-CoS map.
cos-mutation	(Optional) Displays the CoS-mutation map.
dscp-exp	(Optional) Displays the DSCP-to-exp map.
dscp-mutation	(Optional) Displays the DSCP-mutation map.
exp-dscp	(Optional) Displays the exp-to-DSCP map.
exp-mutation	(Optional) Displays the exp-mutation map.
ip-prec-dscp	(Optional) Displays the IP-precedence-to-DSCP map.
policed-dscp	(Optional) Displays the policed-DSCP map.

Command Default All platform QoS maps are displayed.

Command Modes Privileged EXEC (#)

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

Usage Guidelines Maps are used to generate an internal DSCP value, which represents the priority of the traffic. Use the **show platform qos maps** command without keywords to display all maps.

Examples

The following is sample output from the **show platform qos maps cos-dscp** command displaying the DSCP values to which each CoS value will be mapped:

```
Router# show platform qos maps cos-dscp

Cos-dscp map:
  cos:  0  1  2  3  4  5  6  7
-----
  dscp:  8  8  8  8 24 32 56 56
```

The following is sample output from the **show platform qos maps dscp-cos** command displaying the CoS values to which each DSCP value will be mapped:

```
Router# show platform qos maps dscp-cos

Dscp-cos map:
  dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
-----
  cos:   0  1  1  1  2  2  3  3  4  4  5  6  7
```

This example shows how to display the QoS-map settings:

```
Router# show platform qos maps

Policed-dscp map:
  0  1  2  3  4  5  6  7  8  9
-----
  00:  00 01 02 03 04 05 06 07 08 09
  10:  10 11 12 13 14 15 16 17 18 19
  20:  20 21 22 23 24 25 26 27 28 29
  30:  30 31 32 33 34 35 36 37 38 39
  40:  40 41 42 43 44 45 46 47 48 49
  50:  50 51 52 53 54 55 56 57 58 59
  60:  60 61 62 63

Dscp-cos map:
  0  1  2  3  4  5  6  7  8  9
-----
  00:  00 00 00 00 00 00 00 00 01 01
  10:  01 01 01 01 01 01 02 02 02 02
  20:  02 02 02 02 03 03 03 03 03 03
  30:  03 03 04 04 04 04 04 04 04 04
  40:  05 05 05 05 05 05 05 05 06 06
  50:  06 06 06 06 06 06 07 07 07 07
  60:  07 07 07 07

Cos-dscp map:
  cos:   0  1  2  3  4  5  6  7
-----
  dscp:   0  8 16 24 32 40 48 56

IpPrecedence-dscp map:
  ipprec:  0  1  2  3  4  5  6  7
-----
  dscp:   0  8 16 24 32 40 48 56
```

Router#

In the policed DSCP and DSCP-CoS map displays, the new DSCP or CoS values are shown in the body of the table. The decade of the original DSCP value is shown in the left-side vertical column, and the units digit is in the top row. For example, the DSCP-CoS map indicates that if the original DSCP value is between 32 and 39, the CoS will be set to 4.

The CoS-DSCP and IP precedence-DSCP maps display the DSCP values to which each CoS or IP precedence value will be mapped. For example, the IP precedence-DSCP map indicates that if the original IP precedence value is 3, the DSCP will be set to 24.

This example shows how to verify the configuration of DSCP-mutation mapping:

```
Router# show platform qos maps | begin DSCP mutation
DSCP mutation map mutmap1: (dscp= d1d2)
  d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
  0 :    00 01 02 03 04 05 06 07 08 09
  1 :    10 11 12 13 14 15 16 17 18 19
  2 :    20 21 22 23 24 25 26 27 28 29
  3 :    08 31 32 33 34 35 36 37 38 39
  4 :    40 41 42 43 44 45 46 47 48 49
<...Output Truncated...>
Router#
```

In the DSCP mutation map display, the marked-down DSCP values are shown in the body of the table. The first digit (d1) of the original DSCP value is in the left-side vertical column labeled d1, and the second digit (d2) is in the top row. For example, a DSCP value of 30 maps to a new DSCP value of 08.

Related Commands

Command	Description
platform qos map	Defines the CoS-to-DSCP map and DSCP-to-CoS map.
platform qos map cos-dscp	Defines the ingress CoS-to-DSCP map for trusted interfaces.
platform qos map cos-mutation	Maps a packet's CoS to a new CoS value.
platform qos map dscp-cos	Defines an egress DSCP-to-CoS map.
platform qos map dscp-mutation	Defines a named DSCP mutation map.
platform qos map ip-prec-dscp	Defines an ingress IP precedence-to-DSCP map for trusted interfaces.
platform qos map policed-dscp	Sets the mapping of policed DSCP values to marked-down DSCP values.

show platform redundancy

To display platform-specific Constellation WAN (CWAN) redundancy information, use the **show platform redundancy** command in privileged EXEC mode.

```
show platform redundancy { atm | bias | ccb slot-number cpu-number | cwpa-ce3 | cwpa-ct3 |
cwpa-e1 | cwpa-stm1 | cwpa-t1 | frame-relay | hdlc | if-config { slot-number cpu-number
[bay-number] | default-retvals } | mlp | multilink-vc | osm-chocx | osm-ct3 | ppp | shadowstate
| spa-chocx | spa-ct3 | switchover }
```

Syntax	Description
atm	Displays CWAN ATM redundancy state information.
bias	Configures platform redundancy boot bias.
ccp	Displays the CWAN Configuration Control Block (CCB) list.
<i>slot-number</i>	Slot number.
<i>cpu-number</i>	CPU number.
cwpa-ce3	Displays CWAN port adapter (CWPA) Channelized E3 (CE3) redundancy state information.
cwpa-ct3	Displays CWPA-CT3 redundancy state information.
cwpa-e1	Displays CWPA-E1 redundancy state information.
cwpa-stm1	Displays CWPA Synchronous Transport Module level-1 (STM-1) virtual circuit (VC) information.
cwpa-t1	Displays CWPA-T1 redundancy state information.
frame-relay	Displays CWAN Frame Relay redundancy state information.
hdlc	Displays CWAN High-Level Data Link Control (HDLC) redundancy state information.
if-config	Displays the CWAN IF-configuration list.
<i>bay-number</i>	(Optional) Shared Port Adapter (SPA) bay number.
default-retvals	Displays default IF-configuration return values.
mlp	Displays CWAN Multilink Point-to-Point Protocol (MLP) redundancy state information.
multilink-vc	Displays CWAN Multilink VC information.
osm-chocx	Displays CWAN Optical Services Module (OSM) Channelized OC-12/OC-3 line card (CHOCX) redundancy state information.
osm-ct3	Displays CWAN OSM-CT3 redundancy state information.
ppp	Displays CWAN PPP redundancy state information.
shadowstate	Displays the CWAN interface descriptor block (IDB) shadow state.
spa-chocx	Displays CHOCX SPA VC information.
spa-ct3	Displays CT3 SPA VC information.
switchover	Displays CWAN switchover redundancy information.

Command Default None

Command Modes Privileged EXEC (#)

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

Examples The following is sample output from the **show platform redundancy** command with the **if-config** keyword. The fields are self-explanatory.

```
Router# show platform redundancy if-config 4 0

Current number of elements = 0
Current maximum elements = 128
List was grown = 0 times
Number of elements sorted = 0
List errors = 0
List flags = 0x1E
Current element pointer = 0x0
List pointer = 0x50A27438
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| C=Command T=Type P=Port t=timedOut D=Dirty S=Sync      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| C | T | P | key address | t | D | S | value |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

Related Commands	Command	Description
	show platform	Displays platform information.

show platform software acl

To display platform software ACL, use the **show platform software acl** command.

```
show platform software acl { accounting-tbl { index number } | acct-xlt-tbl { in { index number } |
out { index number } } | appid { in number | out number } | capmap { tcam { A { index | module }
| B { index | module } } } | cm-readiness { module } | compaction { detail { module } | label
{ tcam { A | B } } | module number } | entry { module } | label { tcam { A | B } } | lou { index number
| module number } | tcam { count { module } } | tcp-flags-tbl { detail { module } | index number
| module number } | v6-extnhdr-tbl { detail | index | module } }
```

Syntax Description

accounting-tbl	Specifies the accounting table.
index number	Specifies the accounting index. Range is 0–4095.
acct-xlt-tbl	Specifies the accounting table.
in	Specifies the in Acct Xlt entries. Index value Range is 0–255.
out	Specifies the out Acct Xlt entries. Index value Range is 0–255.
appid	Specifies the ACL application ID shadow show commands.
in number	Specifies the in application ID entries. Range is 1–4294967295.
out number	Specifies the out application ID entries. Range is 1–4294967295.
capmap	Specifies the software cap map entries.
tcam	Specifies the software cap map entries.
A	Specifies the entries in cap map A.
B	Specifies the entries in cap map B.
module	Specifies the module.
cm-readiness	Specifies the CM readiness for requests.
compaction	Specifies the software compaction contents.
detail	Specifies the software compaction contents in detail.
label	Specifies the software compaction contents for label.
entry	Specifies the ACL entry matching a pattern (CPU intensive).
lou	Specifies the software LOU contents. Index value range is 0–103.
count	Specifies the software TCAM count.
tcp-flags-tbl	Specifies the software tcp-flags table. Index value range is 0–15.
v6-extnhdr-tbl	Specifies the software v6-extn-hdr table.
detail	Specifies the v6 extension hdr table detail.

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 display platform software ACL application ID Acct-Xlt in entry 4:

```
Router# show platform software acl appid in 4
```

Related Commands

Command	Description
platform software acl	Configures the platform software ACL.

show platform software debug

To display platform software debug logging details, use the **show platform software debug** command.

show platform software debug

Syntax Description This command has no arguments or keywords.

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 display the platform software debug logging details:

```
Router# show platform software debug
```

Related Commands	Command	Description
	platform software debug	Configures the platform software debug logging details.

show platform software e8-recovery

To display platform software EARL8 print recovery patch settings and occurrences, use the **show platform software e8-recovery** command.

show platform software e8-recovery { **config** | **counter** | **data** | **history** }

Syntax Description	Option	Description
	config	Specifies print recovery patch settings.
	counter	Specifies print recovery patch occurrences traffic counter.
	data	Specifies print recovery patch occurrences register data.
	history	Specifies print recovery patch occurrences.

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 display the platform EARL8 software print recovery patch settings:

```
Router# show platform software e8-recovery config
```

Related Commands	Command	Description
	platform software e8-recovery	Configures the platform EARL8 software print recovery patch settings and occurrences.

show platform software earl layer2

To display platform software EARL Layer 2 related information, use the **show platform software earl layer2** command.

```
show platform software earl layer2 {etherchannel {bpm-table {bridge-domain value}} |
l2-opt_stp_purge {clear | dump}}
```

Syntax Description		
etherchannel		Specifies Layer 2 EtherChannel forwarding related information.
bpm-table		Specifies the Bundle Port Map table.
bridge-domain <i>value</i>		Specifies the bridge domain value. Range is 1–16384.
l2-opt_stp_purge		Specifies the count of purging per port.
clear		Clears the counter.
dump		Dumps the counter.

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 display the cleared purged ports per counter in the platform software EARL Layer 2 configuration:

```
Router# show platform software earl layer2 l2-opt_stp_purge clear
```

Related Commands	Command	Description
	platform software earl layer2	Configures the platform software EARL Layer 2 related information.

show platform software fabric

To display platform software crossbar switching fabric-related information, use the **show platform software fabric** command.

```
show platform software fabric {errors | serdes {info {module number} | supervisor slot} |
state-machine {channel {event_trace number | state number} | linecard {event_trace
number | state number}}} | timeout}
```

Syntax Description

errors	Specifies the fabric errors.
serdes	Specifies the fabric SerDes database commands.
info	Specifies information about a fabric SerDes configuration database.
module number	Specifies the module number. Range is 1–6.
supervisor slot	Specifies the supervisor card number. 0 for first supervisor slot and 1 for second supervisor slot.
state-machine	Specifies the state machine for fabric.
channel	Specifies the state machine per channel.
event_trace number	Specifies the last events traversed. Range is 0–25.
state number	Specifies the present state of channel state machines. Range is 0–25.
linecard	Specifies the state machine per line card.
timeout	Specifies the fabric timeout error.

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 display the fabric timeout errors:

```
Router# show platform software fabric timeout
```

Related Commands

Command	Description
platform software fabric	Configures the platform software crossbar switching fabric.

show platform software feature-manager acg-v4

To display feature manager IPv4 access group-specific information on the platform software, use the **show platform software feature-manager acg-v4** command.

```
show platform software feature-manager acg-v4 {all | 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}}
```

Syntax	Description
all	Specifies IPv4 Access-group information on all interfaces.
interface	Specifies interface related information.
<i>async number</i>	Specifies the asynchronous interface number. Range is 1–999.
<i>auto-template number</i>	Specifies the auto-template interface number. Range is 1–999.
<i>ctunnel number</i>	Specifies the Ctunnel interface number. Range is 0–2147483647.
<i>dialer number</i>	Specifies the dialer interface number. Range is 0–255.
<i>esconphy number</i>	Specifies the esconPhy interface number. Range is 1–6.
<i>filter number</i>	Specifies the filter interface number. Range is 1–6.
<i>filtergroup number</i>	Specifies the filter group interface number. Range is 1–6.
<i>gigabitethernet number</i>	Specifies the gigabit Ethernet interface number. Range is 1–6.
<i>longreachethernet number</i>	Specifies the long-reach Ethernet interface number. Range is 1–6.
<i>loopback number</i>	Specifies the loopback interface number. Range is 1–2147483647.
<i>mfr number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
<i>multilink number</i>	Specifies the multilink-group interface number. Range is 1–2147483647.
<i>null number</i>	Specifies the null interface number. Range is 0–0.
<i>port-channel number</i>	Specifies the Ethernet channel of interfaces. Range is 1–496.
<i>portgroup number</i>	Specifies the portgroup interface number. Range is 1–6.
<i>pos-channel number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
<i>sysclock number</i>	Specifies the telecom-bus Clock Controller interface number. Range is 1–6.
<i>tengigabitethernet number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
<i>tunnel number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
<i>vif number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
<i>virtual-template number</i>	Specifies the virtual template interface number. Range is 1–200.
<i>virtual-tokenring number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.

<i>vlan vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
<i>fcpa number</i>	Specifies the fibre channel interface number. Range is 1–6.
<i>control-plane number</i>	Specifies the control plane interface number. Range is 1–6.
<i>voabypassin number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
<i>voabypassout number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
<i>voafilterin number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
<i>voafilterout number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
<i>voain number</i>	Specifies the VOA in interface number. Range is 1–6.
<i>voaout number</i>	Specifies the VOA out interface 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 display the IPv4 access group information on all interfaces:

```
Router# show platform software feature-manager acg-v4 all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager IPv4 access group-specific information on the platform software.

show platform software feature-manager arp-acl

To display feature manager Address Resolution Protocol (ARP) Access Control List (ACL)-specific information on the platform software, use the **show platform software feature-manager arp-acl** command.

```
show platform software feature-manager arp-acl {all | interface {vlan number}}
```

Syntax Description		
	all	Specifies ARP ACL information on all interfaces.
	interface	Specifies interface-related information.
	vlan <i>number</i>	Specifies the Catalyst switch VLAN 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 display the ARP ACL information on all interfaces:

```
Router# show platform software feature-manager arp-acl all
```

Related Commands	Command	Description
	clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager cm-requests

To display feature manager requests or responses sent to CM on the platform software, use the **show platform software feature-manager cm-requests** command.

show platform software feature-manager cm-requests

Syntax Description This command has no arguments or keywords.

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 display the feature manager requests/responses sent to CM:

```
Router# show platform software feature-manager cm-requests
```

Related Commands	Command	Description
	clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager cts-l3s

To display feature manager CTS Layer 3 simplified information on the platform software, use the **show platform software feature-manager cts-l3s** command.

```
show platform software feature-manager cts-l3s {all | 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}}
```

Syntax	Description
all	Specifies feature manager CTS layer 3 simplified information on all interfaces.
interface	Specifies interface-related feature manager CTS Layer 3 simplified information.
async <i>number</i>	Specifies the asynchronous interface number. Range is 1–999.
auto-template <i>number</i>	Specifies the auto-template interface number. Range is 1–999.
ctunnel <i>number</i>	Specifies the Ctunnel interface number. Range is 0–2147483647.
dialer <i>number</i>	Specifies the dialer interface number. Range is 0–255.
esconphy <i>number</i>	Specifies the esconPhy interface number. Range is 1–6.
filter <i>number</i>	Specifies the filter interface number. Range is 1–6.
filtergroup <i>number</i>	Specifies the filter group interface number. Range is 1–6.
gigabitethernet <i>number</i>	Specifies the gigabit Ethernet interface number. Range is 1–6.
longreachethernet <i>number</i>	Specifies the long-reach Ethernet interface number. Range is 1–6.
loopback <i>number</i>	Specifies the loopback interface number. Range is 1–2147483647.
mfr <i>number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink <i>number</i>	Specifies the multilink-group interface number. Range is 1–2147483647.
null <i>number</i>	Specifies the null interface number. Range is 0–0.
port-channel <i>number</i>	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup <i>number</i>	Specifies the portgroup interface number. Range is 1–6.
pos-channel <i>number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom-bus Clock Controller interface number. Range is 1–6.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.

virtual-tokenring <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the feature manager CTS Layer 3 simplified information on all interfaces:

```
Router# show platform software feature-manager cts-13s all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager dai

To display feature manager Dynamic ARP Inspection (DAI)-specific information on the platform software, use the **show platform software feature-manager dai** command.

```
show platform software feature-manager dai {all | interface {vlan number}}
```

Syntax Description		
	all	Specifies DAI information on all interfaces.
	interface	Specifies interface-related information.
	vlan <i>number</i>	Specifies the Catalyst switch VLAN number. Range is 1–4094.

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 display the DAI information on all interfaces:

```
Router# show platform software feature-manager dai all
```

Related Commands	Command	Description
	clear platform software feature-manager	Clears featuremanager-specific information on the platform software.

show platform software feature-manager dhcp-snooping

To display feature manager Dynamic Host Configuration Protocol (DHCP) snooping-specific information on the platform software, use the **show platform software feature-manager dhcp-snooping** command.

show platform software feature-manager dhcp-snooping {all | interface {vlan number}}

Syntax Description		
	all	Specifies DHCP snooping information on all interfaces.
	interface	Specifies interface-related information.
	vlan <i>number</i>	Specifies the Catalyst switch VLAN number. Range is 1–4094.

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 display the DHCP snooping information on all interfaces: Router# show platform software feature-manager dhcp-snooping all
----------	---

Related Commands	Command	Description
	clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager features

To display feature manager features-specific information on the platform software, use the **show platform software feature-manager features** command.

show platform software feature-manager features {brief}

Syntax Description	brief	Displays brief information about all interfaces.
---------------------------	-------	--

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 display brief information about all interfaces:

```
Router# show platform software feature-manager features brief
Interface: Control Plane Interface IP is disabled; admin_state is up
  hw_state[INGRESS] = not reduced, hw_state[EGRESS] = not reduced
  mcast = 0
  priority = 0
  flags = 0x0
  parent[INGRESS] = none
  outbound label: 2
    Feature IP_QOS_EGRESS:
    Feature IPV6_QOS_EGRESS:
    Feature OTHER_QOS_EGRESS:
    Feature ARP_QOS_EGRESS:
    Feature MPLS_QOS_EGRESS:
Interface: Control Plane Interface.1 IP is disabled; admin_state is up
  hw_state[INGRESS] = not reduced, hw_state[EGRESS] = not reduced
  mcast = 0
  priority = 0
  flags = 0x0
  parent[INGRESS] = none
  outbound label: 1
    Feature GRE Tunnel Decapsulation:
    Feature Tunnel Decapsulation:
    Feature IPv6 GRE Tunnel Decapsulation:
    Feature IPv6 Tunnel Decapsulation:
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager fie

To display Feature Interaction Engine (FIE)-specific information on the feature manager, use the **show platform software feature-manager fie** command.

```
show platform software feature-manager fie {all | app-req-state | appid {protocol | shadow protocol} | feat-index | fidb | fie-shadow {feat-index | interface | nf-recirc {all | appid number}} | flowmask {detail} | 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} | label {number | stats {all}} | mergetable | oir {module number} | profile {protocol | shadow protocol} | shadowlabel number | summary}
```

Syntax	Description
all	Specifies FIE status on all interfaces.
app-req-state	Specifies FIE application request state table.
appid	Specifies the application ID. Range is 1–20000.
<i>protocol</i>	Specifies the type of protocol. Range is 0–3. 0=IPv4, 1=IPv6, 2=Layer 2, 3=MPLS.
shadow protocol	Specifies the shadow application ID database. Range is 0–3. 0=IPv4, 1=IPv6, 2=Layer 2, 3=MPLS.
feat-index	Specifies the FIE feat index allocation information.
fidb	Specifies the FIE description block status.
fie-shadow	Specifies the FIE shadow state.
feat-index	Specifies the FIE shadow feat index allocation state.
interface	Displays the available interfaces.
nf-recirc	Specifies the FIE shadow nf-recirc state.
flowmask	Specifies the FIE flow mask status.
detail	Specifies the FIE flow mask detail status.
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 <i>number</i>	Specifies the loopback interface number. Range is 1–2147483647.
mfr <i>number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink <i>number</i>	Specifies the multilink-group interface number. Range is 1–2147483647.
null <i>number</i>	Specifies the null interface number. Range is 0–0.
port-channel <i>number</i>	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup <i>number</i>	Specifies the portgroup interface number. Range is 1–6.
pos-channel <i>number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom-bus Clock Controller interface number. Range is 1–6.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.
virtual-tokenring <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface number. Range is 1–6.
label <i>number</i>	Specifies FIE label information. Range is 1–20000.
stats	Specifies FIE VMR MD5 statistics.
mergetable	Specifies feature merging table information.
oir	Specifies FIE OIR information. Range is 1–6.
module <i>number</i>	Specifies the state of the module number. Range is 1–6.
profile	Specifies profile information.
shadowlabel <i>number</i>	Specifies FIE shadow label information. Range is 1–20000.
summary	Speacfies FIE summary.

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 display the platform feature manager FIE summary:

```
Router# show platform software feature-manager fie summary
```

Related Commands

Command	Description
clear platform software feature-manager fie	Clears the configuration for platform software-specific feature manager FIE.

show platform software feature-manager interface

To display feature manager interface-specific information on the platform software, use the **show platform software feature-manager interface** command.

```
show platform software feature-manager 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}
```

Syntax Description

async <i>number</i>	Specifies the asynchronous interface number. Range is 1–999.
auto-template <i>number</i>	Specifies the auto-template interface number. Range is 1–999.
ctunnel <i>number</i>	Specifies the Ctunnel interface number. Range is 0–2147483647.
dialer <i>number</i>	Specifies the dialer interface number. Range is 0–255.
esconphy <i>number</i>	Specifies the esconPhy interface number. Range is 1–6.
filter <i>number</i>	Specifies the filter interface number. Range is 1–6.
filtergroup <i>number</i>	Specifies the filter group interface number. Range is 1–6.
gigabitethernet <i>number</i>	Specifies the gigabit Ethernet interface number. Range is 1–6.
longreachethernet <i>number</i>	Specifies the long-reach Ethernet interface number. Range is 1–6.
loopback <i>number</i>	Specifies the loopback interface number. Range is 1–2147483647.
mfr <i>number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink <i>number</i>	Specifies the multilink-group interface number. Range is 1–2147483647.
null <i>number</i>	Specifies the null interface number. Range is 0–0.
port-channel <i>number</i>	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup <i>number</i>	Specifies the portgroup interface number. Range is 1–6.
pos-channel <i>number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom-bus Clock Controller interface number. Range is 1–6.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.
virtual-tokenring <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.

control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the feature manager information on all interfaces:

```
Router# show platform software feature-manager interface voaout 4
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager ip-admission

To display feature manager IP admission-specific information on the platform software, use the **show platform software feature-manager ip-admission** command.

```
show platform software feature-manager ip-admission layer2 {all | 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}}
```

```
show platform software feature-manager ip-admission layer3 {all | 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}}
```

Syntax Description

layer2	Specifies IP admission Layer 2-specific information.
layer3	Specifies IP admission Layer 3-specific information.
all	Specifies IP admission information on all interfaces.
interface	Specifies interface related information.
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 <i>number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom-bus Clock Controller interface number. Range is 1–6.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.
virtual-tokenring <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the IP admission information on all Layer 2 interfaces:

```
Router# show platform software feature-manager ip-admission layer2 all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager ip-recirculate

To display feature manager IP recirculate-specific information on the platform software, use the **show platform software feature-manager ip-recirculate** command.

```
show platform software feature-manager ip-recirculate {all | 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}}
```

Syntax Description

all	Specifies IP recirculate information on all interfaces.
interface	Specifies interface related information.
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 <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the IP recirculate information on all interfaces:

```
Router# show platform software feature-manager ip-recirculate all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager ipv6

To display feature manager IPv6-specific information on the platform software, use the **show platform software feature-manager ipv6** command.

```
show platform software feature-manager ipv6 pacl {all | brief | 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}}
```

```
show platform software feature-manager ipv6 rpf {all | 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}}
```

```
show platform software feature-manager ipv6 traffic-filter {all | 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}}
```

Syntax Description

pacl	Specifies IPv6 PACL specific information.
rpf	Specifies feature manager IPv6 RPF specific information.
traffic-filter	Specifies feature manager IPv6 traffic filter specific information.
all	Specifies IPv6 PACL information on all interfaces.
brief	Specifies IPv6 PACL information on all interfaces in brief.
interface	Specifies interface related information.
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 <i>number</i>	Specifies the gigabit Ethernet interface number. Range is 1–6.
longreachethernet <i>number</i>	Specifies the long-reach Ethernet interface number. Range is 1–6.
loopback <i>number</i>	Specifies the loopback interface number. Range is 1–2147483647.
mfr <i>number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink <i>number</i>	Specifies the multilink-group interface number. Range is 1–2147483647.
null <i>number</i>	Specifies the null interface number. Range is 0–0.
port-channel <i>number</i>	Specifies the Ethernet channel of interfaces. Range is 1–496.
portgroup <i>number</i>	Specifies the portgroup interface number. Range is 1–6.
pos-channel <i>number</i>	Specifies the PoS channel of interfaces. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom-bus Clock Controller interface number. Range is 1–6.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.
virtual-tokenring <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the IPv6 PACL information on all interfaces:

```
Router# show platform software feature-manager ipv6 pacl all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager label

To display feature manager label-specific information on the platform software, use the **show platform software feature-manager label** command.

show platform software feature-manager label *{number}*

Syntax Description	<i>number</i>	Specifies the virtual label number. Range is 1–2000.
---------------------------	---------------	--

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 display the label information:

```
Router# show platform software feature-manager label 1
Label 1:
  Hardware state is Not Reduced
  Force merge is FALSE
  Protocol number 0:
    Protocol switching is enabled
    Configured features:
      GRE Tunnel Decapsulation (egress)
      Tunnel Decapsulation (egress)
  Protocol number 1:
    Protocol switching is enabled
    Configured features:
      IPv6 GRE Tunnel Decapsulation (egress)
      IPv6 Tunnel Decapsulation (egress)
  Interfaces (I/E = Ingress/Egress; * = associate pending)
    E Control Plane Interface.1
```

Related Commands	Command	Description
	clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager nat

To display feature manager Network Address Translation (NAT)-specific information on the platform software, use the **show platform software feature-manager nat** command.

```
show platform software feature-manager nat {all | 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} | netflow }
```

Syntax Description

all	Specifies NAT information on all interfaces.
interface	Specifies interface related information.
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 <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface number. Range is 1–6.
netflow	Specifies NAT related netflow data.

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 display the NAT information on all interfaces:

```
Router# show platform software feature-manager nat all
```

Related Commands	Command	Description
	clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager netflow

To display feature manager NetFlow specific information on the platform software, use the **show platform software feature-manager netflow** command.

```
show platform software feature-manager netflow {counters | pattern | slotinfo}
```

Syntax Description

counters	Specifies feature manager NetFlow counters
pattern	Specifies feature manager NetFlow pattern.
slotinfo	Specifies feature manager NetFlow slot 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 display the NetFlow information for counters:

```
Router# show platform software feature-manager netflow counters
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager pacl

To display feature manager access group specific information on the platform software, use the **show platform software feature-manager pacl** command.

```
show platform software feature-manager pacl {all | 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}}
```

Syntax	Description
all	Specifies access group information on all interfaces.
interface	Specifies interface related information.
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 <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the PACL information on all interfaces:

```
Router# show platform software feature-manager pacl all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager pbr

To display feature manager Policy-Based Routing (PBR) specific information on the platform software, use the **show platform software feature-manager pbr** command.

```
show platform software feature-manager pbr {all | 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}}
```

Syntax	Description
all	Specifies PBR information on all interfaces.
interface	Specifies interface related information.
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 <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the PBR information on all interfaces:

```
Router# show platform software feature-manager pbr all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager private-hosts

To display feature manager private hosts-specific information on the platform software, use the **show platform software feature-manager private-hosts** command.

```
show platform software feature-manager private-hosts {all | 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}}
```

Syntax	Description
all	Specifies private hosts information on all interfaces.
interface	Specifies interface related information.
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 <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the private hosts information on all interfaces:

```
Router# show platform software feature-manager private-hosts all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager rdt-indices

To display feature manager redirect LDL indices specific information on the platform software, use the **show platform software feature-manager rdt-indices** command.

show platform software feature-manager rdt-indices

Syntax Description This command has no arguments or keywords.

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 display the redirect LDL indices information on all interfaces:

```
Router# show platform software feature-manager rdt-indices
```

Related Commands	Command	Description
	clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager rpf

To display feature manager RPF-specific information on the platform software, use the **show platform software feature-manager rpf** command.

```
show platform software feature-manager rpf {all | 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}}
```

Syntax Description

all	Specifies RPF information on all interfaces.
interface	Specifies interface related information.
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 <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the RPF information on all interfaces:

```
Router# show platform software feature-manager rpf all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager scl

To display feature manager SCL-specific information on the platform software, use the **show platform software feature-manager scl** command.

```
show platform software feature-manager scl {all | brief | 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} | netflow }
```

Syntax Description

all	Specifies SCL information on all interfaces.
brief	Specifies SCL information on all interfaces in brief.
interface	Specifies interface related information.
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 <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 None.

Examples This example shows how to display the SCL information on all interfaces:

```
Router# show platform software feature-manager scl all
```

Related Commands	Command	Description
	clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager summary

To display the feature manager summary on the platform software, use the **show platform software feature-manager summary** command.

```
show platform software feature-manager summary {}
```

Syntax Description This command has no arguments or keywords.

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 display the feature manager summary information:

```
Router# show platform software feature-manager summary
```

Related Commands	Command	Description
	clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager sve

To display feature manager SVE-specific information on the platform software, use the **show platform software feature-manager sve** command.

```
show platform software feature-manager sve {all | brief | 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} | netflow}
```

Syntax	Description
all	Specifies SVE information on all interfaces.
brief	Specifies SVE information on all interfaces in brief.
interface	Specifies interface related information.
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 <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the SVE information on all interfaces:

```
Router# show platform software feature-manager sve all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager tcp-mss

To display feature manager TCP MSS adjust-specific information on the platform software, use the **show platform software feature-manager tcp-mss** command.

```
show platform software feature-manager tcp-mss {all | 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}}
```

Syntax	Description
all	Specifies TCP MSS information on all interfaces.
interface	Specifies interface related information.
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 <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the TCP-MSS information on all interfaces:

```
Router# show platform software feature-manager tcp-mss all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager vACL

To display feature manager VACL-specific information on the platform software, use the **show platform software feature-manager vACL** command.

```
show platform software feature-manager vACL {all | 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}}
```

Syntax	Description
all	Specifies VACL information on all interfaces.
interface	Specifies interface related information.
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 <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the VACLformation on all interfaces:

```
Router# show platform software feature-manager vac1 all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software feature-manager wccp

To display feature-manager WCCP-specific information on the platform software, use the **show platform software feature-manager wccp** command.

```
show platform software feature-manager wccp {all | inband | 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}}
```

Syntax	Description
all	Specifies WCCP information on all interfaces.
inband	Specifies inband-related WCCP information.
interface	Specifies interface related information.
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 <i>number</i>	Specifies the virtual token ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the fibre channel interface number. Range is 1–6.
control-plane <i>number</i>	Specifies the control plane interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass-in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass-out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter-in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter-out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface 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 display the WCCP information on all interfaces:

```
Router# show platform software feature-manager wccp all
```

Related Commands

Command	Description
clear platform software feature-manager	Clears feature manager-specific information on the platform software.

show platform software flow internal

To display information on platform software flow internal, use the **show platform software flow internal** command.

```
show platform software flow internal {mgmt statistics | search statistics | fnf statistics | export
statistics | driver statistics | api statistics | em statistics | am statistics | tt statistics | yn
statistics | cli statistics | interrupt statistics | ehsa statistics}
```

Syntax Description		
	mgmt statistics	Specifies management statistics.
	search statistics	Specifies search statistics.
	fnf statistics	Specifies FNF statistics.
	export statistics	Specifies export statistics.
	driver statistics	Specifies driver statistics.
	api statistics	Specifies API statistics.
	em statistics	Specifies EM statistics.
	am statistics	Specifies AM statistics.
	tt statistics	Specifies TT statistics.
	yn statistics	Specifies YN statistics.
	cli statistics	Specifies CLI statistics.
	interrupt statistics	Specifies interrupt statistics.
	ehsa statistics	Specifies EHSA 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 display platform software flow internal management statistics:

```
Router# show platform software flow internal mgmt statistics
```

Related Commands

Command	Description
clear platform software flow internal	Clears information on platform software flow internal.

show platform software lif l2

To display platform software Layer 2 LIF information, use the **show platform software lif l2** command.

```
show platform software lif l2 {api_statistics {clear | dump} | idbhal{bitlist | status} |
  pthread_lock | queue {api | idbhal | pm | tml} | shadow {total} | table {bd number {all | total}
  | port number {all | total}| vlan vlan_id {all | total}}}
```

Syntax	Description
api_statistics	Specifies the LDB API statistics.
clear	Clears the LDB API statistics.
dump	Dumps the LDB API statistics.
idbhal	Specifies the shadow LDB entries.
bitlist	Specifies the LDB bit list.
status	Specifies the LDB IDBHAL status.
pthread_lock	Specifies the Pthread Lock.
queue	Specifies the queue information.
api	Specifies the API events.
pm	Specifies the PM events.
tml	Specifies the TML events.
shadow	Specifies the shadow LDB entries.
total	Specifies the total number of entries in the database.
table	Specifies the software tables.
bd number	Specifies the hardware BD number. Range is 0–16383.
all	Specifies all the entries.
port number	Specifies the port number. Range is 0–16383.
vlan vlan_id	Specifies the VLAN ID. Range is 0–4095.

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 display platform software LIF Layer 2 API statistics that are cleared:

```
Router# show platform software lif l2 api_statistics clear
```

Related Commands

Command	Description
platform software lif 12	Configures the platform software for Layer 2 LIF.

show platform software lif l3

To display platform software Layer 3 LIF information, use the **show platform software lif l3** command.

```
show platform software lif l3 {api_stats {display {module number} | reset {module}} | block
number | handle number | icc_stats {display {module} | reset{module}} | index number |
inheritance{egress {module} | ingress {module}} | mem_stats {display {module} | reset
{module}} | mtu{table {dump{module} | index number}} | region {all {module} | id number
| summary {module}} | special {module} | tml_stats {display {module}}}
```

Syntax Description

api_stats	Specifies the API library statistics information.
display	Displays LIF API library statistics information.
module number	Specifies the module for the command. Range 1–6.
reset	Resets LIF API library statistics information.
block	Specifies the software LIF block information. Range is 0–1023.
handle number	Specifies the LIF handle. Range is 0– 4294967295.
icc_stats	Specifies the ICC statistics information.
index number	Specifies the LIF index. Range is 0–1048575.
inheritance	Specifies the LIF region based inheritance information.
egress	Specifies the software LIF egress inheritance information.
ingress	Specifies the software LIF ingress inheritance information.
mem_stats	Specifies the memory statistics information.
display	Displays LIF memory statistics information.
reset	Resets LIF memory statistics information.
mtu	Specifies the MTU information.
table	Specifies the software MTU table information.
dump	Dumps the software LIF Layer 3 MTU table.
index number	Specifies the software MTU table information. Range is 0– 63.
region	Specifies the software LIF region information.
all	Specifies information about the software LIF for all region ids.
id number	Specifies information about the software LIF region IDs. Range is 0–63.
summary	Specifies the software LIF region summary information.
special	Specifies the software LIF special entry information.
tml_stats	Specifies the TML statistics information.
display	Displays LIF TML library statistics information.

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 display platform software LIF Layer 3 API statistics for module 4:

```
Router# show platform software lif l3 api_stats display module 4
```

Related Commands

Command	Description
platform software lif l3	Configures the platform software for Layer 3 LIF.

show platform software lif stats

To display platform software LIF statistics, use the **show platform software lif stats** command.

```
show platform software lif stats {agg {bdindex number | index number} | index number |
interface {gigabitethernet number | port-channel number | tengigabitethernet number |
tunnel number | vlan vlan_id}}
```

Syntax Description		
agg		Specifies the software aggregate LIF statistics information.
bdindex number		Specifies the LIF BD index. Range is 0–16383.
index number		Specifies the LIF statistics index. Range is 0–131071.
index number		Specifies the LIF index. Range is 0–131071.
interface		Specifies the interface name.
gigabitethernet number		Specifies the Gigabit Ethernet IEEE 802.3z. Range is 1–6.
port-channel number		Specifies the Ethernet channel interface. Range is 1–496.
tengigabitethernet number		Specifies the 10-Gigabit Ethernet. Range is 1–6.
tunnel number		Specifies the tunnel interface. Range is 0–2147483647.
vlan vlan_id		Specifies the Catalyst VLANs. Range is 1–4094.

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 display platform software aggregate LIF statistics information for BD index 4:

```
Router# show platform software lif stats agg bdindex 4
```

Related Commands	Command	Description
	platform software lif stats	Configures the platform software LIF statistics.

show platform software ltl

To display platform LTL software information, use the **show platform software ltl** command.

```
show platform software ltl {allocation | assigned | callback | regions | router | span |
well-known-index}
```

Syntax Description

allocation	Displays LTL software allocation information.
assigned	Displays LTL software-assigned region usage information.
callback	Displays LTL software port callback information.
regions	Displays LTL regions information.
router	Displays router port presence.
span	Displays SPAN port presence.
well-known-index	Displays LTL software regions WKI 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 display the platform software LTL regions information:

```
Router# show platform software ltl regions
```

Related Commands

Command	Description
platform software ltl	Configures the platform software LTL.

show platform software met

To display platform software MET-related information, use the **show platform software met** command.

show platform software met {detail | statistics | summary}

Syntax Description	Option	Description
	detail	Displays detailed MET information.
	statistics	Displays MET statistics information.
	summary	Displays MET summary 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 display platform software MET information in detail:

```
Router# show platform software met detail
```

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

show platform software met detail

To display software information for the multicast expansion table (MET), use the **show platform software met detail** command in privileged EXEC mode.

show platform software met detail

Syntax Description This command has no keywords or arguments.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines

Examples This example shows how to display software routing for the MET:

```
Router# show platform software met detail
Replication Engine(s) in Slot : 5
MET start address: 0x4
MET end address: 0x7FFE
MET total entries: 32744
MET free entries: 14

Total MET sets: 8
Total references: 8
Total oifs: 10

MET allocation profile: [10% size 2, 30% size 4, 50% size 8, 10% size 16]

BD Flood Mgr Client Information:
=====
Client ID: 1
MET sets: 0
References: 0
Oifs: 0
```

Related Commands	Command	Description
	debug platform software multicast routing	Displays information about multicast errors.
	platform software met profile	Configures the number of blocks for each block size of your MET profile.

Command	Description
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 oir

To display platform software OIR information, use the **show platform software oir** command.

```
show platform software oir {debug {all number | mask number | oir_mask number | stdby_reset
| swover_data_path_mask number | swover_global_mask number | swover_time_mask
number} | pmb {registers number} | seq-sync-info number | state-machine number}
```

Syntax Description		
debug		Displays the debug information.
all <i>number</i>		Displays all saved information by module number. Range is 1–6.
mask <i>number</i>		Specifies a mask to select information. Range is 0–255.
oir_mask <i>number</i>		Specifies OIR mask to select information. Range is 1–6.
stdby_reset		Specifies standby reset tracebacks.
swover_data_path_ mask <i>number</i>		Specifies switchover data path mask. Range is 1–6.
swover_global_mask <i>number</i>		Specifies switchover global mask. Range is 1–6.
swover_time_mask <i>number</i>		Specifies switchover time mask. Range is 1–6.
pmb		Displays the PMB related registers.
registers <i>number</i>		Specifies the register number. Range is 1–6.
seq-sync-info <i>number</i>		Displays the pinnacle synchronization problem related registers. Range is 1–6.
state-machine <i>number</i>		Displays the last state machine transition. 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 display the platform software OIR debug information for mask 4:

```
Router# show platform software oir debug mask 4
```

Related Commands

Command	Description
platform software oir	Configures the platform software OIR.

show platform software stub

To display platform software stub-related information, use the **show platform software stub** command.

```
show platform software stub {all | traceback {disable {stub-function-id number} | enable
{stub-function-id number}} | used}
```

Syntax Description		
all		Displays all stubs.
traceback		Specifies disabling or enabling traceback.
disable		Specifies disabling traceback.
stub-function-id <i>number</i>		Specifies a stub function ID number. Range is 0–49.
enable		Specifies enabling traceback.
used		Displays the stubs that were called upon.

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 display the platform software stub disabled traceback with stub function ID 4:

```
Router# show platform software stub traceback disable stub-function-id 4
```

Related Commands	Command	Description
	platform software stub	Configures the platform software stubs.

show platform software xconnect

To display platform software xConnect configuration details, use the **show platform software xconnect** command.

```
show platform software xconnect {circuit-index {all | 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 | fcpa number |
voabypassin number | voabypassout number | voafilterin number | voafilterout number |
voain number | voaout number}} | mac-addr | pstats}
```

Syntax Description

circuit-index	Displays the Layer 2 circuit index information.
all	Displays all information on all Layer 2 circuit indices.
interface	Lists the various interfaces on Layer 2 circuit indices to choose from.
async <i>number</i>	Specifies the asynchronous interface number. Range is 1–999.
auto-template <i>number</i>	Specifies the auto-template interface number. Range is 1–999.
ctunnel <i>number</i>	Specifies the channel tunnel interface number. Range is 0–2147483647.
dialer <i>number</i>	Specifies the dialer interface number. Range is 0–255.
esconphy <i>number</i>	Specifies the EsconPhy interface number. Range is 1–6.
filter <i>number</i>	Specifies the filter interface number. Range is 1–6.
filtergroup <i>number</i>	Specifies the filter group interface number. Range is 1–6.
gigabitethernet <i>number</i>	Specifies the Gigabit Ethernet interface number. Range is 1–6.
longreachethernet <i>number</i>	Specifies the long-reach Ethernet interface number. Range is 1–6.
loopback <i>number</i>	Specifies the loopback interface number. Range is 1–2147483647.
mfr <i>number</i>	Specifies the multilink Frame Relay bundle interface number. Range is 1–2147483647.
multilink <i>number</i>	Specifies the multilink group interface number. Range is 1–2147483647.
null <i>number</i>	Specifies the null interface number. Range is 0–0.
port-channel <i>number</i>	Specifies the Ethernet channel interface. Range is 1–496.
portgroup <i>number</i>	Specifies the Port group interface number. Range is 1–6.
pos-channel <i>number</i>	Specifies the POS channel interface. Range is 1–4094.
sysclock <i>number</i>	Specifies the telecom-bus clock controller interface number. Range is 1–6.
tengigabitethernet <i>number</i>	Specifies the 10-Gigabit Ethernet interface number. Range is 1–6.
tunnel <i>number</i>	Specifies the tunnel interface number. Range is 1–2147483647.
vif <i>number</i>	Specifies the PGM multicast host interface number. Range is 1–1.
virtual-template <i>number</i>	Specifies the virtual template interface number. Range is 1–200.

virtual-tokenring <i>number</i>	Specifies the virtual Token Ring interface number. Range is 1–2147483647.
vlan <i>vlan_id</i>	Specifies the VLAN interface number. Range is 1–4094.
fcpa <i>number</i>	Specifies the Fibre Channel interface number. Range is 1–6.
voabypassin <i>number</i>	Specifies the VOA bypass in interface number. Range is 1–6.
voabypassout <i>number</i>	Specifies the VOA bypass out interface number. Range is 1–6.
voafilterin <i>number</i>	Specifies the VOA filter in interface number. Range is 1–6.
voafilterout <i>number</i>	Specifies the VOA filter out interface number. Range is 1–6.
voain <i>number</i>	Specifies the VOA in interface number. Range is 1–6.
voaout <i>number</i>	Specifies the VOA out interface number. Range is 1–6.
mac-addr	Specifies the proxy ARP MAC address.
pstats	Specifies the packet statistics.

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 display the platform software xConnect packet statistics:

```
Router# show platform software xconnect pstats
```

Related Commands

Command	Description
platform software xconnect	Configures platform software xConnect.

show platform supervisor

To display platform supervisor information, use the **show platform supervisor** command in privileged EXEC mode.

```
show platform supervisor mtu slot slot-number port port-number
```

Syntax Description	mtu	Displays supervisor operating maximum transmission unit (MTU).
	slot slot-number	Displays information for the specified slot.
	port port-number	Displays information for the specified port.

Command Default None

Command Modes Privileged EXEC (#)

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

Examples The following is sample output from the **show platform supervisor** command. The fields are self-explanatory.

```
Router# show platform supervisor mtu slot 5 port 1

User configured MTU : 9216
Real Operating MTU : 9236
```

Related Commands	Command	Description
	show platform	Displays platform information.

show platform supervisor mtu

To display information on platform supervisor operating MTU, use the **show platform supervisor mtu** command.

show platform supervisor mtu {slot *number*}

Syntax Description	slot <i>number</i>	Specifies the slot 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	<p>This example shows how to display information on platform supervisor operating MTU slot 4:</p> <pre>Router# show platform supervisor mtu slot 5</pre>
-----------------	--

Related Commands	Command	Description
	platform supervisor mtu	Configures the platform supervisor operating MTU.

show vlan group

To display the VLANs mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

```
show vlan group [group-name group-name] [user-count]
```

Syntax Description	group-name	(Optional) Displays the VLANs mapped to the specified VLAN group.
	<i>group-name</i>	
user-count	(Optional) Displays the user count of the group's VLANs.	

Defaults This command has no default settings.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SX11	Support for this command was introduced.
	12.2(50)SY	Added user-count keyword.

Usage Guidelines The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If the **group-name** keyword is entered, only the members of the VLAN group specified by the *group-name* argument are displayed.

Examples This example shows how to display the members of a specified VLAN group:

```
Router# show vlan group group-name ganymede
```

```
Group Name Vlans Mapped
```

```
-----  
ganymede          7-9
```

```
Router#
```

This example shows how to display the user count for a specified group:

```
Router# show vlan group group-name ganymede user-count
```

```
VLAN      : Count
```

```
-----  
3         : 0
```

```
4         : 0
```

```
5         : 0
```

```
Router#
```

Related Commands	Command	Description
	vlan group	Creates or modifies a VLAN group.

snmp-server enable traps errdisable

To enable the CISCO-ERR-DISABLE-MIB Simple Network Management Protocol (SNMP) notification for traps and informs, use the **snmp-server enable traps errdisable** command in global configuration mode. To disable errdisable notifications, use the **no** form of this command.

snmp-server enable traps errdisable [notification-rate *rate*]

no snmp-server enable traps [notification-rate *rate*]

Syntax Description	notification-rate <i>rate</i> (Optional) Sets the number of notifications per minute.
---------------------------	--

Command Default	SNMP notifications are disabled.
------------------------	----------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(33)SX14	Support for this command was introduced.
	12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Examples	This example shows how to enable the SNMP errdisable notifications:
-----------------	---

```
Router(config)# snmp-server enable traps errdisable
Router(config)#
```

This example shows how to set the SNMP errdisable notification rate to 500 per minute:

```
Router(config)# snmp-server enable traps errdisable notification-rate 500
Router(config)#
```

Related Commands	Command	Description
	test snmp trap errdisable ifevent	Tests the cErrDisableInterfaceEventRev1 trap.

snmp-server enable traps power-ethernet

To enable Simple Network Management Protocol (SNMP) power ethernet trap notifications, use the **snmp-server enable traps power-ethernet** command in global configuration mode. To disable PPPoE session count SNMP notifications, use the **no** form of this command.

snmp-server enable traps power-ethernet group *number*

no snmp-server enable traps power-ethernet group *number*

Syntax Description	group <i>number</i> Sets the group number; valid values are 1 to 13.
---------------------------	---

Command Default	SNMP notifications are disabled.
------------------------	----------------------------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	12.2(33)SJX2	This command was introduced.
	15.1(1)SY	This command was introduced.

Usage Guidelines	This command enables SNMP traps only. It does not support inform requests.
-------------------------	--

Examples	The following example shows how to set the notifications for power-ethernet group 3:
-----------------	--

```
Router(config)# snmp-server enable traps power-ethernet group 3
```

snmp-server enable traps trustsec-sxp

To enable the sending of CISCO-TRUSTSEC-SXP-MIB traps on Simple Network Management Protocol (SNMP), use the **snmp-server enable traps trustsec-sxp** command in global configuration mode. To disable all available SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps trustsec-sxp [binding-conflict | binding-err | binding-expn-fail |
conn-config-err | conn-down | conn-srcaddr-err | conn-up | msg-parse-err |
oper-nodeid-change]
```

```
no snmp-server enable traps trustsec-sxp [binding-conflict | binding-err | binding-expn-fail |
conn-config-err | conn-down | conn-srcaddr-err | conn-up | msg-parse-err |
oper-nodeid-change]
```

Syntax Description

binding-conflict	(Optional) Enables ctsxSxpBindingConflictNotif notifications.
binding-err	(Optional) Enables ctsxSxpBindingErrNotif notifications.
binding-expn-fail	(Optional) Enables ctsxSxpBindingExpnFailNotif notifications.
conn-config-err	(Optional) Enables ctsxSxpConnConfigErrNotif notifications.
conn-down	(Optional) Enables ctsxSxpConnDownNotif notifications.
conn-srcaddr-err	(Optional) Enables ctsxSxpConnSourceAddrErrNotif notifications.
conn-up	(Optional) Enables ctsxSxpConnUpNotif notifications.
msg-parse-err	(Optional) Enables ctsxSxpMsgParseErrNotif notifications.
oper-nodeid-change	(Optional) Enables ctsxSxpOperNodeIdChangeNotif notifications.

Defaults

No notifications controlled by this command are sent.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

If you do not specify any of the optional keywords, all TrustSec SXP notifications are enabled.

The **snmp-server enable traps snmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to enable ctsxSxpBindingConflictNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp binding-conflict
```

The following example shows how to enable the router to enable ctsxSxpBindingErrNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp binding-err
```

The following example shows how to enable the router to enable ctsxSxpBindingExpnFailNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp binding-expn-fail
```

The following example shows how to enable the router to enable ctsxSxpConnConfigErrNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp conn-config-err
```

The following example shows how to enable the router to enable ctsxSxpConnDownNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp conn-down
```

The following example shows how to enable the router to enable ctsxSxpConnUpNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp conn-up
```

The following example shows how to enable the router to enable ctsxSxpMsgParseErrNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp msg-parse-err
```

The following example shows how to enable the router to enable ctsxSxpConnConfigErrNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp conn-config-err
```

The following example shows how to enable the router to enable ctsxSxpOperNodeIdChangeNotif notifications:

```
Router(config)# snmp-server enable traps trustsec-sxp oper-nodeid-change
```

Related Commands

Command	Description
test snmp trap trustsec	test snmp trap trustsecTests CISCO-TRUSTSEC-MIB traps.
test snmp trap trustsec-interface	test snmp trap trustsec-interfaceTests CISCO-TRUSTSEC-INTERFACE-MIB traps.
test snmp trap trustsec-policy	test snmp trap trustsec-policyTests CISCO-TRUSTSEC-POLICY-MIB traps.
test snmp trap trustsec-server	test snmp trap trustsec-serverTests CISCO-TRUSTSEC-SERVER-MIB traps.

switch pmk

To enable VSL on the switch, use the **switch pmk** command in Privileged EXEC mode. To disable VSL use the **no** form of the command.

switch pmk *hex-data*

no switch pmk *hex-data*

Syntax Description	<i>hex-data</i>	Pairwise Master Key (PMK) without the leading 0x.
--------------------	-----------------	---

Defaults	None
----------	------

Command Modes	Privileged EXEC mode
---------------	----------------------

Command History	Release	Modification
	15.0(1)SY1	This command was introduced.

Usage Guidelines	You must enter an even number of hexadecimal characters or prefix the last character with a zero.
------------------	---

Examples	This example shows how to enable VSL on a switch:
----------	---

```
Switch(config-vs-domain) switch pmk
Switch(config-vs-domain) #
```

Examples	This example shows how to disable VSL on a switch:
----------	--

```
Switch(config-vs-domain) no switch pmk
Switch(config-vs-domain) #
```

Related Commands	Command	Description
	vsl-encryption	Configures VSL encryption on the switch.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

```
switchport trunk {encapsulation dot1q | native vlan | allowed vlan}
```

```
no switchport trunk {encapsulation dot1q | native vlan | allowed vlan}
```

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

```
switchport trunk {encapsulation {isl | dot1q [ethertype value] | negotiate}} | { native vlan {tag | vlan-id}} | {allowed vlan vlan-list} | {pruning vlan vlan-list}
```

```
no switchport trunk {encapsulation {isl | dot1q [ethertype value] | negotiate} | native vlan [tag] | allowed vlan | pruning vlan}
```

Syntax Description

encapsulation isl	Sets the trunk encapsulation format to Inter-Switch Link (ISL).
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
native vlan	Sets the native VLAN for the trunk in 802.1Q trunking mode.
allowed vlan <i>vlan-list</i>	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
ethertype <i>value</i>	(Optional) Sets the EtherType value; valid values are from 0x0 to 0x5EF-0xFFFF.
encapsulation negotiate	Specifies that if the Dynamic Inter-Switch Link (DISL) protocol and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan tag	Enables the native VLAN tagging state on the interface.
native vlan <i>vlan-id</i>	The particular native VLAN.
pruning vlan <i>vlan-list</i>	Sets the list of VLANs that are enabled for VLAN Trunking Protocol (VTP) pruning when the interface is in trunking mode. See the “Usage Guidelines” section for the <i>vlan-list</i> argument formatting guidelines.

Defaults

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

- The default encapsulation type is dot1q.
- The default access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- The default for all VLAN lists is to include all VLANs.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

- The encapsulation type is dependent on the platform or interface hardware.
- The access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.

- The default for all VLAN lists is to include all VLANs.
- **ethertype** *value* for 802.1Q encapsulation is 0x8100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	Support for this command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(17a)SX	This command was modified to include the following: <ul style="list-style-type: none"> • Restriction of ISL trunk-encapsulation. • Addition of the dot1q keyword and ethertype <i>value</i> keyword and argument.
12.2(18)SXD	This command was modified to allow the switchport trunk allowed vlan command to be entered on interfaces where the span destination port is either a trunk or an access port.
12.2(18)SXE	This command was modified to remove support for Gigabit Ethernet (GE) Optimized Layer 2 WAN ports.
12.2(33)SXH	This command was modified to allow the tagging of native VLAN traffic on a per-port basis.
12.2(33)SXI4	This command was modified to allow the switchport trunk command to only be applied on the port channel (PO) itself.
12.2(50)SY	This command was modified to remove the isl and negotiate keywords in Cisco IOS Release 12.2(50)SY.

Usage Guidelines**802.1Q Trunks**

- When you connect Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning-tree loops. Cisco recommends that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree bridge protocol data units (BPDUs) on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Shared Spanning Tree Protocol (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- The 802.1Q switches that are not Cisco switches maintain only a single instance of spanning-tree (Mono Spanning Tree [MST]) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a switch through an 802.1Q trunk without a Cisco switch, the MST of the switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning-tree topology known as the Common Spanning Tree (CST).

- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, switches that are not Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the 802.1Q cloud receive these flooded BPDUs. This condition allows Cisco switches to maintain a per-VLAN spanning-tree topology across a cloud of 802.1Q switches that are not Cisco switches. The 802.1Q cloud of switches separating the Cisco switches is treated as a single broadcast segment among all switches connected to the 802.1Q cloud of switches that are not Cisco switches through 802.1Q trunks.
- Make sure that the native VLAN is the same on *all* of the 802.1Q trunks that connect the Cisco switches to the 802.1Q cloud of switches that are not Cisco switches.
- If you are connecting multiple Cisco switches to a 802.1Q cloud of switches that are not Cisco switches, all of the connections must be through 802.1Q trunks. You cannot connect Cisco switches to an 802.1Q cloud of switches that are not Cisco switches through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning-tree “port inconsistent” state and no traffic will pass through the port.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support 802.1Q formats.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** *vlan-list*[,*vlan-list*...] where:

- **all**—Specifies all VLANs from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.
- **none**—Indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** form of the command.
- **add**—Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove**—Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except**—Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *vlan-list*—Is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

This command is not supported on GE Layer 2 WAN ports.

You can enter the **switchport trunk** command only on the PO. If you enter the **switchport trunk** command on a port member the following message is displayed:

```
Configuration is not allowed on Port members. Remove the interface from the Port Channel
to modify its config
```

The **switchport trunk encapsulation dot1q** command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats. Only 802.1Q encapsulation is supported by shared port adapters (SPAs).

The **switchport trunk encapsulation isl** command is not supported in Cisco IOS Release 12.2(50)SY.

If you enter the **switchport trunk encapsulation isl** command on a port channel containing an interface that does not support ISL-trunk encapsulation, the command is rejected.

You can enter the **switchport trunk allowed vlan** command on interfaces where the span destination port is either a trunk or an access port.

You can enter the **switchport trunk native vlan tag** command to enable the tagging of native VLAN traffic on a per-port basis. When tagging is enabled, all the packets on the native VLAN are tagged and all incoming untagged data packets are dropped, but untagged control packets are accepted. When tagging is disabled, the native VLAN packets going out on trunk ports are not tagged and the incoming untagged packets are allowed and assigned to the native VLAN. The **no switchport trunk native vlan tag** command overrides the **vlan dot1q tag native** command for global tagging.

**Note**

The **switchport trunk native vlan tag** interface configuration mode command does not enable native VLAN tagging unless you first configure the switch to tag native VLAN traffic globally. To enable native VLAN tagging globally, use the **vlan dot1q tag native** command in global configuration mode.

**Note**

The **switchport trunk pruning vlan** *vlan-list* command does not support extended-range VLANs; valid *vlan-list* values are from 1 to 1005.

The **dot1q ethertype** *value* keyword and argument are not supported on port-channel interfaces. You can enter the command on the individual port interface only. Also, you can configure the ports in a channel group to have different EtherType configurations.

The **switchport trunk encapsulation negotiate** command is not supported in Cisco IOS Release 12.2(50)SY.

**Caution**

Be careful when configuring the custom EtherType value on a port. If you enter the **negotiate** keyword and DISL and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, then ISL is the selected format and may pose as a security risk. The **no** form of this command resets the trunk-encapsulation format to the default.

- The **no** form of the **switchport trunk native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.
- The **no** form of the **switchport trunk native vlan tag** command configures the Layer 2 port not to tag native VLAN traffic.
- The **no** form of the **switchport trunk allowed vlan** command resets the list to the default list, which allows all VLANs.
- The **no** form of the **switchport trunk pruning vlan** command resets the list to the default list, which enables all VLANs for VTP pruning.
- The **no** form of the **switchport trunk encapsulation dot1q ethertype** *value* command resets the list to the default value.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** [*vlan-list* [, *vlan-list* ...]] where:

- **all**—Specifies all the appropriate VLANs. This keyword is not supported in the **switchport trunk pruning vlan** command.
- **none**—Indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** command.
- **add** *vlan-list* [, *vlan-list* ...]—Adds the defined list of VLANs to those currently set instead of replacing the list.

- **remove** *vlan-list*[,*vlan-list*...]—Removes the defined list of VLANs from those currently set instead of replacing the list. You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic (for example, Cisco Discovery Protocol, version 3; VTP; Port Aggregation Protocol, version 4 (PAgP4); and DTP) in VLAN 1.



Note You can remove any of the default VLANs (1002 to 1005) from a trunk; this action is not allowed in earlier releases.

- **except** *vlan-list*[,*vlan-list*...]—Excludes the specified list of VLANs from those currently set instead of replacing the list.
- *vlan-list*[,*vlan-list*...]—Specifies a single VLAN number from 1 to 4094 or a continuous range of VLANs that are described by two VLAN numbers from 1 to 4094. You can specify multiple VLAN numbers or ranges of numbers using a comma-separated list.

To specify a range of VLANs, enter the smaller VLAN number first, separated by a hyphen and the larger VLAN number at the end of the range.

Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Cisco 7600 series router running the Cisco IOS software on both the supervisor engine and the Multilayer Switch Feature Card (MSFC) to a Cisco 7600 series router running the Catalyst operating system. These VLANs are reserved in Cisco 7600 series routers running the Catalyst operating system. If enabled, Cisco 7600 series routers running the Catalyst operating system may disable the ports if a trunking channel is between these systems.

Examples

The following example shows how to cause a port interface configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Router(config-if)# switchport trunk encapsulation dot1q
```

The following example shows how to configure the Layer 2 port to tag native VLAN traffic:

```
Router(config-if)# switchport trunk native vlan tag
```

Related Commands

Command	Description
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
vlan dot1q tag native	Enables dot1q tagging for all VLANs in a trunk.

test platform software console disconnect-timeout

To test the platform software timeout after physically disconnecting a console port, use the **test platform software console disconnect-timeout** command.

test platform software console disconnect-timeout *time*

Syntax Description	<i>time</i>	Specifies the time in seconds; valid values are 1 through 10.
---------------------------	-------------	---

Defaults	Disabled and 1 second.	
-----------------	------------------------	--

Command Modes	Privileged EXEC mode	
----------------------	----------------------	--

Command History	Release	Modification
	15.1(1)SY	Support for this command was introduced.
15.1(2)SY	Update Defaults updated.	

Examples	This example shows how to set the disconnect timeout test to 4 seconds:	
-----------------	---	--

```
Router# test platform software console disconnect-timeout 4
```

Related Commands	Command	Description
	disconnect-timeout	Changes the EXEC timeout value for the main console after the console cable is removed.

test snmp trap errdisable ifevent

To test CISCO-ERR-DISABLE-MIB cErrDisableInterfaceEventRev1 Simple Network Management Protocol (SNMP) traps and informs, use the **test snmp trap errdisable ifevent** command in privileged EXEC mode.

test snmp trap errdisable ifevent

Syntax Description This command has no keywords or arguments.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(33)SX14	Support for this command was introduced.
	12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Examples This example shows the output of **test snmp trap errdisable ifevent** when snmp-server enable traps errdisable is not configured:

```
Router# test snmp trap errdisable ifevent
cErrDisableInterfaceEventRev1 notification is disabled.
Router#
```

This example shows the output of **test snmp trap errdisable ifevent** when snmp-server enable traps errdisable is configured:

```
Router# test snmp trap errdisable ifevent
cErrDisableInterfaceEventRev1 notification was sent.
Router#
```

Related Commands	Command	Description
	snmp-server enable traps errdisable	Enables SNMP errdisable notifications.

test snmp trap trustsec-server provision-secret

To test ctsvNoProvisionSecretNotif traps, use the **test snmp trap trustsec-server provision-secret** command in privileged EXEC mode.

```
test snmp trap trustsec-server provision-secret
```

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC mode

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

Examples This example shows how to the ctsvNoProvisionSecretNotif traps:

```
Router# test snmp trap trustsec-server provision-secret
```


test snmp trap trustsec-server radius-server

To test ctsvNoRadiusServerNotif traps, use the **test snmp trap trustsec-server radius-server** command in privileged EXEC mode.

test snmp trap trustsec-server radius-server

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC mode

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

Examples This example shows how to the ctsvNoRadiusServerNotif traps:

```
Router# test snmp trap trustsec-server radius-server
```

test snmp trap trustsec-sxp

To test CISCO-TRUSTSEC-SXP-MIB traps on Simple Network Management Protocol (SNMP), use the **test snmp trap trustsec-sxp** command in Exec mode.

```
test snmp trap trustsec-sxp [binding-conflict | binding-err | binding-expn-fall | conn-config-err
| conn-down | conn-sraddr-err | conn-up | msg-parse-err | oper-nodeid-change]
```

Syntax Description	
binding-conflict	(Optional) Enables ctsxSxpBindingConflictnotif notifications.
binding-err	(Optional) Enables ctsxSxpBindingErrnotif notifications.
binding-expn-fall	(Optional) Enables ctsxSxpBindingExpnFailNotif notifications.
conn-config-err	(Optional) Enables ctsxSxpConnConfigErrNotif notifications.
conn-down	(Optional) Enables ctsxSxpConnDownNotif notifications.
conn-sraddr-err	(Optional) Enables ctsxSxpConnSourceAddrErrnotif notifications.
conn-up	(Optional) Enables ctsxSxpConnUpNotif notifications.
msg-parse-err	(Optional) Enables ctsxSxpMsgParseErrNotif notifications.
oper-nodeid-change	(Optional) Enables ctsxSxpOperNodeIdChangeNotif notifications.

Command Default Disabled.

Command Modes EXEC mode (#)

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

Usage Guidelines SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

If you do not specify any of the optional keywords, all TrustSec SXP notifications are enabled.

The **snmp-server enable traps snmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples The following example shows how to test the binding conflict MIB:

```
Router# test snmp trap trustsec-sxp binding-conflict
ctsxSxpBindingConflictNotif notification is disabled.
Router#
```

The following example shows how to test the binding err MIB:

```
Router# test snmp trap trustsec-sxp binding-err
ctsxSxpBindingErrNotif notification is disabled.
```

Router#

The following example shows how to test the binding-expn-fail MIB:

```
Router# test snmp trap trustsec-sxp binding-expn-fail
ctsxSxpBindingExpnFailNotif notification is disabled.
Router#
```

The following example shows how to test the conn-config-err MIB:

```
Router# test snmp trap trustsec-sxp conn-config-err
ctsxSxpConnConfigErrNotif notification is disabled.
Router#
```

The following example shows how to test the conn-down MIB:

```
Router# test snmp trap trustsec-sxp conn-down
ctsxSxpConnDownNotif notification is disabled.
Router#
```

The following example shows how to test the conn-srcaddr-err MIB:

```
Router# test snmp trap trustsec-sxp conn-srcaddr-err
ctsxSxpConnSourceAddrErrNotif notification is disabled.
Router#
```

The following example shows how to test the conn-up MIB

```
Router# test snmp trap trustsec-sxp conn-up
ctsxSxpConnUpNotif notification is disabled.
Router#
```

The following example shows how to test the msg-parse-err MIB:

```
Router# test snmp trap trustsec-sxp msg-parse-err
ctsxSxpMsgParseErrNotif notification is disabled.
Router#
```

The following example shows how to test the oper-nodeid-change MIB:

```
Router# test snmp trap trustsec-sxp msg-parse-err
ctsxSxpMsgParseErrNotif notification is disabled.
Router#
```

Related Commands

Command	Description
test snmp trap trustsec	Tests CISCO-TRUSTSEC-MIB traps.
test snmp trap trustsec-interface	Tests CISCO-TRUSTSEC-INTERFACE-MIB traps.
test snmp trap trustsec-policy	Tests CISCO-TRUSTSEC-POLICY-MIB traps.
test snmp trap trustsec-server	Tests CISCO-TRUSTSEC-SERVER-MIB traps.

upgrade hardware database

To upgrade the hardware database, use the **upgrade hardware database** command.

```
upgrade hardware database {file file_name | {preference | invalidate} {region1 | region2} |
    slot slot_number {file file_name | invalidate {region1 | region2}}}
```

Syntax Description

file <i>file_name</i>	Specifies the name of a hardware database file.
preference	Specifies the hardware database boot file.
invalidate	Specifies the hardware database region to invalidate.
region1	Specifies the hardware database region1.
region2	Specifies the hardware database region2.
<i>slot_number</i>	Specifies the slot number of a module that has hardware abstraction layer (HAL) support.

Defaults

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.0(1)SY1	Support for this command was introduced.

Usage Guidelines

This command is useful only if a new hardware database version becomes available.

Examples

This example shows how to upgrade the platform hardware database version:

```
Router# upgrade hardware database file bootdisk:file_name
Router#
*date_and_time: Hardware database upgrade in progress
*date_and_time: Erasing flash
*date_and_time: Programming flash
*date_and_time: Verifying new hardware database
*date_and_time: Hardware database upgrade complete

*date_and_time: The system must be reload for this to take effect
```

Related Commands

Command	Description
show platform hardware database	Displays the platform hardware database version.

upgrade hardware image

To upgrade the hardware image, use the **upgrade hardware image** command.

```
upgrade hardware image slot slot_number {file file_name |
  {preference | invalidate} region_number | reset}
```

Syntax Description	Parameter	Description
	slot <i>slot_number</i>	Specifies the slot number of a module that has hardware abstraction layer (HAL) support.
	file <i>file_name</i>	Specifies the name of a hardware image file.
	preference	Specifies the hardware database boot file.
	invalidate	Specifies the hardware database region to invalidate.
	<i>region_number</i>	Specifies the number of a hardware image region.
	reset	Specifies the slot to reset.

Defaults None

Command Modes Privileged EXEC mode

Command History	Release	Modification
	15.0(1)SY1	Support for this command was introduced.

Usage Guidelines This command is useful only if a new hardware image version becomes available. This command is supported only on modules that have hardware abstraction layer (HAL) support.

Examples This example shows how to upgrade the platform hardware database version:

```
Router# upgrade hardware image slot 4 file bootdisk:file_name
!!! {...} !!!
Linecard must be reset. Please use "upgrade hardware image slot 4 reset" command to reset
linecard.
Router# upgrade hardware image slot 4 reset
Router#
*date_and_time: %OIR-6-SP_REMCARD: Card removed from slot 4, interfaces disabled
*date_and_time: %DIAG-6-RUN_COMPLETE: Module 4: Running Complete Diagnostics..4
*date_and_time: %DIAG-6-DIAG_OK: Module 4: Passed Online Diagnostics
Upgrade XML file complete
Upgrade image file complete
Please wait for automatic linecard reset to make upgrade taking effect
*date_and_time: %OIR-6-SP_INSCARD: Card inserted in slot 4, interfaces are now online
*date_and_time: %OIR-6-SP_REMCARD: Card removed from slot 4, interfaces disabled
*date_and_time: %DIAG-6-RUN_COMPLETE: Module 4: Running Complete Diagnostics...
*date_and_time: %DIAG-6-DIAG_OK: Module 4: Passed Online Diagnostics
*date_and_time: %OIR-6-SP_INSCARD: Card inserted in slot 4, interfaces are now online
```

Related Commands

Command	Description
show platform hardware image version	Displays the platform hardware image version.

upgrade hardware transceiver xml

To upgrade the hardware transceiver xml version, use the **upgrade hardware transceiver xml** command.

```
upgrade hardware transceiver xml { file file_name | { preference | invalidate } region_number }
```

Syntax Description		
file <i>file_name</i>	Specifies the name of a transceiver xml file.	
preference	Specifies the hardware dateabase boot file.	
invalidate	Specifies the hardware database region to invalidate.	
<i>region_number</i>	Specifies the number of a transceiver xml region.	

Defaults	
	None

Command Modes	
	Privileged EXEC mode

Command History	Release	Modification
	15.0(1)SY1	Support for this command was introduced.

Usage Guidelines	
	This command is useful only if a new hardware transceiver xml version becomes available.

Examples	
	This example shows how to upgrade the platform hardware database version:

```
Router# upgrade hardware transceiver xml file bootdisk:file_name
Transceiver XML is upgraded successfully
Please unplug and replug supported transceiver
Router#
```

Related Commands	Command	Description
	show platform hardware transceiver xml version	Displays the platform hardware transceiver xml version.

upgrade hardware xml slot

To upgrade the hardware xml version, use the **upgrade hardware xml slot** command.

```
upgrade hardware xml slot slot_number {file file_name |
preference | invalidate} region_number | reset}
```

Syntax Description		
<i>slot_number</i>	Specifies the slot number of a module that has hardware abstraction layer (HAL) support.	
file <i>file_name</i>	Specifies the name of a transceiver xml file.	
preference	Specifies the hardware dateabase boot file.	
invalidate	Specifies the hardware database region to invalidate.	
<i>region_number</i>	Specifies the number of a transceiver xml region.	
reset	Specfies the slot to reset.	

Defaults None

Command Modes Privileged EXEC mode

Command History	Release	Modification
	15.0(1)SY1	Support for this command was introduced.

Usage Guidelines This command is useful only if a new hardware xml version becomes available.
 This command is supported only on modules that have hardware abstraction layer (HAL) support.

Examples This example shows how to upgrade the platform hardware xml version:

```
Router# upgrade hardware xml slot 4 file bootdisk:file_name
Linecard must be reset. Please use "upgrade hardware xml slot 4 reset" command to reset linecard.
Router# upgrade hardware xml slot 4 reset

Upgrade XML file complete
Please wait for automatic linecard reset to make upgrade taking effect

*date_and_time: %OIR-6-SP_INSCARD: Card inserted in slot 4, interfaces are now online
*date_and_time: %OIR-6-SP_REMCARD: Card removed from slot 4, interfaces disabled

*date_and_time: %OIR-6-SP_INSCARD: Card inserted in slot 4, interfaces are now online
Router#
```


Related Commands

Command	Description
show platform hardware xml version	Displays the platform hardware xml version.

vlan access-log

To configure the VLAN access control list (VACL)-logging properties, including the log-table size, redirect-packet rate, and logging threshold, use the **vlan access-log** command in global configuration. To return to the default settings, use the **no** form of this command.

```
vlan access-log { maxflow max-number | ratelimit pps | threshold pkt-count }
```

```
no vlan access-log { maxflow | ratelimit | threshold }
```

Syntax Description

maxflow <i>max-number</i>	Specifies the maximum log-table size. Valid values are from 0 to 2048; 0 deletes the contents of the log table.
ratelimit <i>pps</i>	Specifies the maximum redirect VACL-logging packet rate; valid values are from 0 to 5000.
threshold <i>pkt-count</i>	Specifies the logging-update threshold; valid values are from 0 to 2147483647. 0 means that the threshold is not set.

Command Default

The defaults are as follows:

- *max-number* is **500**.
- *pps* is **2000** pps in Cisco IOS 12.2SX releases.
- *pps* is **0** pps in Cisco IOS release 12.2(50)SY and later.
- *pkt-count* is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY. Added a new default for the ratelimit keyword.

Usage Guidelines

Due to the rate-limiting function for redirected packets, VACL-logging counters may not be accurate. Only denied IP packets are logged.

When the log-table size is full, the logging packets from the new flows are dropped by the software.

The packets that exceed the maximum redirect VACL-logging packet rate limit are dropped by the hardware.

A logging message is displayed if the flow threshold is reached before the 5-minute interval.

If you do not configure the maximum log-table size, maximum packet rate, or threshold, or if you enter the **no** form of the commands, the default values are assumed.

Examples

This example shows how to set the maximum log-table size:

```
Router(config)# vlan access-log maxflow 500  
Router(config)#
```

This example shows how to set the maximum redirect VACL-logging packet rate after which packets are dropped:

```
Router(config)# vlan access-log ratelimit 200  
Router(config)#
```

This example shows how to set the logging-update threshold:

```
Router(config)# vlan access-log threshold 3500  
Router(config)#
```

Related Commands

Command	Description
show vlan access-log	Displays information about the VACL logging including the configured logging properties.

vsl-encryption

To configure VSL encryption on the switch, use the **vsl-encryption** command in Virtual switch domain mode, use the **no** form of the command to disable VSL encryption.

vsl-encryption

no vsl-encryption

Syntax Description This command has no keywords or arguments.

Defaults None

Command Modes Virtual switch domain mode

Command History	Release	Modification
	15.0(1)SY1	This command was introduced.

Usage Guidelines You do not need to enable FIPs before you enable VSL encryption; however if you intend to use FIPs you should enable VSL encryption first.

Examples This example shows how to enable VSL encryption on a switch:

```
Switch(config-vs-domain) vsl-encryption
Switch(config-vs-domain) #
```

This example shows how to disable VSL encryption on a switch:

```
Switch(config-vs-domain) no vsl-encryption
Switch(config-vs-domain) #
```

Related Commands	Command	Description
	switch pmk	Enables VSL on the switch.

wrr-queue bandwidth

To allocate the bandwidth between the standard transmit queues, use the **wrr-queue bandwidth** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

wrr-queue bandwidth *weight-1 ... weight-n*

no wrr-queue bandwidth

Syntax Description

weight-1 ... weight-n WRR weights; valid values are from 1 to 255.

Defaults

The defaults are as follows:

- QoS enabled—4:255
- QoS disabled—255:1

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced.
12.2(17a)SX	This command was changed to support seven queue weights.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

You can configure up to seven queue weights on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

You can configure up to three queue weights on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

WRR allows bandwidth sharing at the egress port. This command defines the bandwidths for egress WRR through scheduling weights. Four queues participate in the WRR unless you enable the egress-expedite queue. The expedite queue is a strict-priority queue that is used until it is empty before using one of the WRR queues.

There is no order of dependencies for the **wrr-queue bandwidth** command. If you enable the egress priority, the weight ratio is calculated with the first two and the last parameters; otherwise, all four parameters are used.

The WRR weights are used to partition the bandwidth between the queues if all queues are nonempty. For example, entering weights of 1:3 means that one queue gets 25 percent of the bandwidth and the other queue gets 75 percent as long as both queues have data.

Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# wrr-queue bandwidth 3 1
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue queue-limit	Sets the transmit-queue size ratio on an interface.

wrr-queue cos-map

To map CoS values to drop thresholds for a queue, use the **wrr-queue cos-map** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
wrr-queue cos-map queue-id threshold-id cos-1 ... cos-n
```

```
no wrr-queue cos-map
```

Syntax Description

<i>queue-id</i>	Queue number; the valid values are from 1 to 2 .
<i>threshold-id</i>	Threshold ID; valid values are from 1 to 2.
<i>cos-1</i> ... <i>cos-n</i>	CoS value; valid values are from 0 to 7.

Defaults

The defaults are as follows:

- Receive queue 1/drop threshold 1 and transmit queue 1/drop threshold 1: CoS 0 and 1.
- Receive queue 1/drop threshold 2 and transmit queue 1/drop threshold 2: CoS 2 and 3.
- Receive queue 2/drop threshold 3 and transmit queue 2/drop threshold 1: CoS 4 and 6.
- Receive queue 2/drop threshold 4 and transmit queue 2/drop threshold 2: CoS 7.
- On 1p1q4t, 1p2q2t, and 1p3q1t interfaces, CoS 5 is mapped to the strict-priority queues.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

Enter up to eight CoS values to map to the threshold.

The threshold for 1p3q1t is always 1.

Examples

This example shows how to map the CoS values 0 and 1 to standard transmit queue 1/threshold 1:

```
Router(config-if)# wrr-queue cos-map 1 1 0 1
```


wrr-queue dscp-map

To map the hardware Differentiated Services Code Point (DSCP) values to the drop threshold values for a queue, use the **wrr-queue dscp-map** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
wrr-queue dscp-map queue-id threshold-id dscp-1 ... dscp-n
```

```
no wrr-queue dscp-map queue-id
```

Syntax Description

<i>queue-id</i>	Queue number; valid values are from 1 to 8.
<i>threshold-id</i>	Threshold ID; valid values are from 1 to 4.
<i>dscp-1 ... dscp-n</i>	DSCP value; valid values are from 0 to 7.

Defaults

The interface is in Class of Service (CoS) mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF5	Support for this command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.



Note To enter the **wrr-queue dscp-map** command, the interface must be in DSCP-queuing mode. Use the **mls qos queue-mode mode-dscp** command to set the mode to DSCP.

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

When mapping DSCP values, follow these guidelines:

- You can enter up to eight DSCP values that map to a queue and threshold.
- You can enter multiple commands to map additional DSCP values to the queue and threshold.
- You must enter a separate command for each queue and threshold.

Examples

This example shows how to map the hardware DSCP values to the drop threshold values for a queue:

```
wrr-queue dscp-map 8 1 0 1 2 3
```

Related Commands

show queueing interface Displays queueing information.

wrr-queue queue-limit

To set the transmit-queue size ratio on an interface, use the **wrr-queue queue-limit** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
wrr-queue queue-limit queue1-weight [queue2-weight] queue3-weight
```

```
no wrr-queue queue-limit
```

Syntax Description		
<i>queue1-weight</i>	Ratio of the low-priority queue weight; valid values are from 1 and 100 percent.	
<i>queue2-weight</i>	(Optional) Ratio of the medium-priority queue weight; valid values are from 1 and 100 percent.	
<i>queue3-weight</i>	Ratio of the high-priority queue weight; see the “Usage Guidelines” section for valid values.	

Defaults

The defaults are as follows:

- 90 percent for low priority
- 10 percent for high priority

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queuing-only** command or the **auto qos default** command is configured.

Valid high-priority weight values are from 1 to 100 percent, except on 1p2q1t egress LAN ports, where valid values for the high-priority queue are from 5 to 100 percent.

On 1p2q2t interfaces, QoS sets the strict-priority queue size equal to the high-priority queue size.

Estimate the mix of low priority-to-high priority traffic on your network (for example, 80 percent low-priority traffic and 20 percent high-priority traffic). Use the estimated percentages as queue weights.

Due to the granularity of programming the hardware, the values that are set in the hardware are close approximations of the provided values. For example, if you specify 0 percent, the actual value that is programmed is not necessarily 0.

Examples

This example shows how to configure the transmit-queue size ratio:

```
Router(config-if)# wrr-queue queue-limit 75 25
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue bandwidth	Allocates the bandwidth between the standard transmit queues.

wrr-queue random-detect

To enable WRED or specify the minimum and maximum WRED threshold for the specified queues on 1p2q2t and 1p3q1t interfaces, use the **wrr-queue random-detect** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
wrr-queue random-detect queue-id
```

```
wrr-queue random-detect {max-threshold | min-threshold} queue-id threshold-percent-1 ...
threshold-percent-n
```

```
no wrr-queue random-detect queue-id
```

```
no wrr-queue random-detect {max-threshold | min-threshold} queue-id
```

Syntax	Description
<i>queue-id</i>	Queue number; valid values are 1, 2, or 3.
max-threshold	Specifies the maximum WRED-drop threshold.
min-threshold	Specifies the minimum WRED-drop threshold.
<i>threshold-percent-1</i> <i>threshold-percent-n</i>	Threshold weights; valid values are from 1 to 100 percent.

Defaults

The default is that WRED is disabled. When WRED is enabled, the defaults are as follows:

- The maximum threshold is (low) 40 percent and (high) 100 percent.
- The minimum thresholds are both set to zero.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

1p2q1t and 1p3q1t interfaces have WRED-drop thresholds in their standard transmit queues. You can configure 1p3q1t transmit queues to use a WRED-drop threshold or a tail-drop threshold.

To enable WRED-drop thresholds on 1p2p1t interfaces, enter the **wrr-queue random-detect** *queue-id* command. Use the **no** form of this command to disable WRED.

To enable WRED-drop thresholds on 1p3q1t interfaces, enter the **wrr-queue random-detect** *queue-id* command. To return to the tail-drop threshold, enter the **no wrr-queue random-detect** *queue-id* command.

The *queue-id* argument is 1 for the standard low-priority queue, 2 for the standard high-priority queue, and 3 for strict priority.

The threshold in the strict-priority queue is not configurable.

Each queue on a 1p2q2t interface has two thresholds; 1p3q1t interfaces have one threshold.

Each threshold has a low and a high WRED value.

WRED values are a percentage of the queue capacity.

For additional information on configuring WRED thresholds, refer to the QoS chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to configure the low-priority transmit-queue high-WRED drop thresholds:

```
Router(config-if)# wrr-queue random-detect max-threshold 1 60 100
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue queue-limit	Sets the transmit-queue size ratio on an interface.

wrr-queue threshold

To configure the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces, use the **wrr-queue threshold** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
wrr-queue threshold queue-id threshold-percent-1 ... threshold-percent-n
```

```
no wrr-queue threshold queue-id
```

Syntax Description

<i>queue-id</i>	Queue number; valid values are 1 and 2.
<i>threshold-percent-1</i>	Number of weights for queues 1 and 2; valid values are from 1 to 100 percent.
<i>threshold-percent-n</i>	

Defaults

When you enable QoS, the default values are as follows:

- **100** percent for threshold 1
- **60** percent for threshold 2

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines



Note

In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

Use the transmit queue and threshold numbers.

The *queue-id* argument is 1 for the standard low-priority queue and 2 for the standard high-priority queue.

Always set threshold 2 to 100 percent.

Receive-queue drop thresholds are supported only on Gigabit Ethernet interfaces that are configured to trust CoS.

Examples

This example shows how to configure receive queue 1/threshold 1 and transmit queue 1/threshold 1:

```
Router(config-if)# wrr-queue threshold 1 60 100
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue queue-limit	Sets the transmit-queue size ratio on an interface.