show ip mds forwarding through show monitor event-trace merged-list

show ip mds forwarding

To display the Multicast Forwarding Information Base (MFIB) table and forwarding information for multicast distributed switching (MDS) on a line card, use the **show ip mds forwarding** command in user EXEC or privileged EXEC mode.

show ip mds forwarding [*group-address*] [*source-address*]

Syntax Description

group-address	(Optional) Address of the IP multicast group for which to display the MFIB table.
source-address	(Optional) Address of the source of IP multicast packets for which to display the MFIB table.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.2(11)GS	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.

Usage Guidelines

Use this command on the line card. This command displays the MFIB table, forwarding information, and related flags and counts.

Note To reach the console for a line card, enter **attach** *slot#*(slot number where the line card resides).

On a Gigabit Switched Router (GSR) only, line card commands can be executed from the Route Processor (RP) using the following syntax: **execute** [**slot** *slot-number* | **all**] *command.*

The *command* argument is any of the line card **show** commands, such as **show ip mds summary** and **show ip mds forward**.

Examples

The following is sample output from the **show ip mds forwarding**command:

```
Router# show ip mds forwarding
IP multicast MDFS forwarding information and statistics:
```

```
Flags: N - Not MDFS switchable, F - Not all MDFS switchable, O - OIF Null
       R - In-ratelimit, A - In-access, M - MTU mismatch, P - Register set
Interface state: Interface, Next-Hop, Mac header
(*, 224.2.170.73),
  Incoming interface: Null
  Pkts: 0, last used: never, Kbps: 0, fast-flags: N
  Outgoing interface list: Null
(172.17.62.86, 224.2.170.73) [31]
  Incoming interface: Fddi3/0/0
  Pkts: 3034, last used: 00:00:00, Kbps: 0, fast-flags: M
  Outgoing interface list:
```

The table below describes the significant fields shown in the display.

Table 1: show ip mds forwarding Field Descriptions

Field	Description
(172.17.62.86, 224.2.170.73) [31])	Source and group addresses. The number in brackets is the hash bucket for the route.
Incoming interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
Pkts	Total number of packets switched by the entry in the table.
last used:	Time when this MFIB entry was used to switch a packet.
Kbps:	Kilobits per second of the switched traffic.
Outgoing interface list	Interfaces through which packets will be forwarded.

show ip mds interface

To display Multicast Distributed Switching (MDS) information for all the interfaces on the line card, use the **show ip mds interface**command in user EXEC or privileged EXEC mode.

show ip mds interface [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Supports the Multicast Virtual Private Network (VPN) routing and forwarding instance (VRF).
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
11.2(11)GS	This command was integrated into Cisco IOS Release 11.2(11)GS.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip mds interface**command:

```
Router# show ip mds interface
Interface                SW-Index  HW-Index  HW IDB      FS Vector   VRF
Ethernet1/0/0            2         1         0x60C2DB40  0x602FB7A4 default
Ethernet1/0/1            3         2         0x60C32280  0x603D52B8 default
Ethernet1/0/2            4         3         0x60C35E40  0x602FB7A4 default
Ethernet1/0/3            5         4         0x60C39E60  0x603D52B8 default
Ethernet1/0/4            6         5         0x60C3D780  0x602FB7A4 default
Ethernet1/0/5            7         6         0x60C41140  0x602FB7A4 default
Ethernet1/0/6            8         7         0x60C453A0  0x602FB7A4 default
Ethernet1/0/7            9         8         0x60C48DC0  0x602FB7A4 default
POS2/0/0                 10        9         0x0                    default
POS3/0/0                 11        10        0x0                    default
```

```
Virtual-Access1          13        11        0x0                   default
Loopback0                14        12        0x0                   default
Tunnel0                  15        23        0x61C2E480  0x603D52B8  vrf1
Tunnel1                  16        24        0x61C267E0  0x603D52B8  vrf2
Ethernet1/0/3.1          17        4         0x60C39E60  0x603D52B8  vrf1
Ethernet1/0/3.2          18        4         0x60C39E60  0x603D52B8  vrf2
```

The table below describes the significant fields shown in the display.

Table 2: show ip mds interface Field Descriptions

Field	Description
Interface	The specified interface.
SW-Index	Software index.
HW-Index	Hardware index.
HW IDB	Hardware interface description block.
FS Vector	Fast Switching Vector.
VRF	VPN routing/forwarding instance.

show ip mds stats

To display multicast distributed switching (MDS) statistics, use the **show ip mds stats** command in user EXEC or privileged EXEC mode.

show ip mds stats {**switching**| **linecard**| **ipc-msg**}

Syntax Description

switching	Displays switching statistics.
linecard	Displays line card statistics.
ipc-msg	Displays Interprocess Communication (IPC) message statistics.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.2(11)GS	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
12.0(33)S	This command was modified. The **ipc-msg** keyword was added.

Usage Guidelines

The **switching** and **linecard** keywords are available only on the Route Processor (RP). The **ipc-msg**keyword is available on both the RP and line card (LC).

Examples

The following is sample output from the **show ip mds stats**command with the **switching**keyword:

```
Router# show ip mds stats switching
Slot Total       Switched    Drops      RPF        Punts      Failures
                                                              (switch/clone)
 1   0           0           0          0          4          0/0
 3   20260925    18014717    253        93         2247454    1/0
```

The table below describes the fields in the display.

Table 3: show ip mds stats switching Field Descriptions

Field	Description
Slot	Slot number for the line card.
Total	Total number of packets received.
Switched	Total number of packets switched.
Drops	Total number of packets dropped.
RPF	Total number of packets that failed reverse path forwarding (RPF) lookup.
Punts	Total number of packets sent to the RP because the line card could not switch them.
Failures (switch/clone)	Times that the RP tried to switch but failed because of lack of resources or clone for the RSP only; failed to get a packet clone.

The following is sample output from the **show ip mds stats**command with the **linecard** keyword:

```
Router# show ip mds stats linecard
Slot      Status    IPC(seq/max) Q(high/route)  Reloads
 1        active    10560/10596      0/0            9
 3        active    11055/11091      0/0            9
```

The table below describes the fields in the display.

Table 4: show ip mds stats linecard Field Descriptions

Field	Description
Slot	Slot number for the line card.
Status	MDS line card status.
IPC(seq/max)	MDS IPC message sequence number and maximum sequence number for the linecard.
Q(high/route)	Length of the high and normal priority MDS IPC queue.
Reloads	The number of MDS downloads that happened in the line card.

The following is sample output from a line card using the **show ip mds stats** command with the **ipc-msg** keyword:

```
Router# show ip mds stats ipc-msg
MDFS IPC stats information
==========================
MDFS Reload stats
-----------------
Full reload request: 1          Partial reload request: 0
LC disable request : 0
MDFS ipc messages sent
----------------------
line card stats    : 494394     mdb stats             : 38421
hwidb stats        : 4775       swidb stats           : 4805
flow control msg   : 6981       clear mroute msg      : 0
MDFS alert messages received
----------------------------
mdfs enable alert  : 306        table2 size alert     : 0
clear all alert    : 206        clear stats alert     : 0
spd alert          : 714        svd alert             : 303
route limit alert  : 4          source limit alert    : 5
punt limit alert   : 707
MDFS ipc messages received
--------------------------
gdb msg  : 431        mdb msg      : 11866      midb msg           : 749592
hwidb msg: 4915       oir hwidb msg: 51         hwidb erase msg    : 51
swidb msg: 5456       oir swidb msg: 51         swidb erase msg    : 51
mdt msg  : 263        rpdf msg     : 0          fwd table erase msg: 0
mdt mgid ext slotmask msg: 6                  mvrf ext slotmask msg: 719
```

The table below describes the fields in the display.

Table 5: show ip mds stats ipc-msg switching Field Descriptions

Field	Description
MDFS Reload stats	
Full reload request	Number of full multicast distributed switching (MDS) download requests sent.
Partial reload request	Number of partial MDS download requests sent.
LC disable request	Number of requests sent to disable MDS on the line card.
MDFS ipc messages sent	
line card stats	Number of line card statistic messages sent.
mdb stats	Number of Multicast Descriptor Block (MDB) statistics messages sent.
hwidb stats	Number of hardware Interface Descriptor Block (HWIDB) statistics messages sent.
swidb stats	Number of software Interface Descriptor Block (SWIDB) statistics messages sent.
flow control msg	Number of flow control messages sent.

Field	Description
clear mroute msg	Number of clear multicast route (mroute) messages sent.
MDFS alert messages received	
mdfs enable alert	Number of multicast distributed fast switching (MDFS) enable alert messages received.
table2 size alert	Number of table2 size alert messages received.
clear all alert	Number of clear all alert messages received.
clear stats alert	Number of clear statistics alert messages received
spd alert	Number of selective packet discard (SPD) alert messages received.
svd alert	Number of singular value decomposition (SVD) alert messages received.
route limit alert	Number of mroute limit alert messages received.
source limit alert	Number of sources per group limit alert messages received.
punt limit alert	Number of MDFS punt limit alert messages received.
MDFS ipc messages received	
gdb msg	Number of GDB messages received.
mdb msg	Number of MDB messages received.
midb msg	Number of multicast interface data block (MIDB) messages received.
hwidb msg	Number of HWIDB messages received.
oir hwidb msg	Number of HWIDB online insertion and removal (OIR) messages received.
hwidb erase msg	Number of HWIDB erase messages received.
swidb msg	Number of SWIDB messages received.
oir swidb msg	Number of SWIDB OIR messages received.
swidb erase msg	Number of SWIDB erase messages received.

Field	Description
mdt msg	Number of Multicast Distribution Tree (MDT) messages received.
rpdf msg	Number of rendezvous point designated forwarder (RPDF) messages received.
fwd table erase msg	Number of MDFS forwarding table erase messages received.
mdt mgid ext slotmask msg	Number of MDFS MDT multicast global identifier (MGID) extended slotmask messages received.
mvrf ext slotmask msg	Number of MDFS Multicast Virtual Routing and Forwarding (MVRF) extended slotmask messages received.

show ip mds summary

To display a summary of the Multicast Forwading Information Base (MFIB) table for multicast distributed switching (MDS), use the **show ip mds summary** command in user EXEC or privileged EXEC mode.

show ip mds summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.2(11)GS	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.

Usage Guidelines

Use this command on a line card. On a Gigabit Switched Router (GSR) only, line card commands can be executed from the Route Pricessor (RP) using the following syntax:

execute [**slot** *slot-number* | **all**] *command*

The *command* argument is any of the line card **show** commands, such as **show ip mds summary** or **show ip mds forward**.

Examples

The following is sample output from the **show ip mds summary**command:

```
Router# show ip mds summary
IP multicast MDFS forwarding information and statistics:
Flags: N - Not MDFS switchable, F - Not all MDFS switchable, O - OIF Null
       R - In-ratelimit, A - In-access, M - MTU mismatch, P - Register set
Interface state: Interface, Next-Hop, Mac header
(*, 224.2.170.73),
  Incoming interface: Null
  Pkts: 0, last used: never, Kbps: 0, fast-flags: N
(172.17.62.86, 224.2.170.73) [31]
  Incoming interface: Fddi3/0/0
  Pkts: 3045, last used: 00:00:03, Kbps: 0, fast-flags: M
(172.22.3.7, 224.2.170.73) [334]
  Incoming interface: Fddi3/0/0
  Pkts: 0, last used: never, Kbps: 0, fast-flags: M
```

The table below describes the significant fields in the display.

Table 6: show ip mds summary Field Descriptions

Field	Description
(172.17.62.86, 224.2.170.73) [31]	Source and group addresses. The number in brackets is the hash bucket for the route.
Incoming interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
Pkts	Total number of packets switched by that entry.
last used	Time when this MFIB entry was used to switch a packet.
Kbps	Kilobits per second of the switched traffic.

show ip traffic

To display the global or system-wide IP traffic statistics for one or more interfaces, use the **show ip traffic** command in user EXEC or privileged EXEC mode.

show ip traffic [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays the global or system-wide IP traffic statistics for a specific interface. If the **interface** keyword is used, the *type* and *number* arguments are required.

Command Default

Using the **show ip traffic**command with no keywords or arguments displays the global or system-wide IP traffic statistics for all interfaces.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2	The output was enhanced to display the number of keepalive, open, update, route-refresh request, and notification messages received and sent by a Border Gateway Protocol (BGP) routing process.
12.2(25)S	The command output was modified.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXH5	This command was modified. The output was changed to display the ARP (proxy) reply counter as the number of ARP replies for real proxies only.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S. This command was modified to include the optional **interface** keyword and associated *type* and *number* arguments. These modifications were made to provide support for the IPv4 MIBs as described in RFC 4293: *Management Information Base for the Internet Protocol (IP)* .

Release	Modification
15.1(4)M	This command was modified. The optional **interface** keyword and associated *type* and *number* arguments were added. These modifications were made to provide support for the IPv4 MIBs as described in RFC 4293, *Management Information Base for the Internet Protocol (IP)* .

Usage Guidelines

Using the **show ip traffic**command with the optional **interface** keyword displays the ipIfStatsTable counters for the specified interface if IPv4 addressing is enabled.

Examples

The following is sample output from the **show ip traffic** command:

```
Router# show ip traffic
IP statistics:
  Rcvd:  27 total, 27 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 27 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  0 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
  Drop:  0 packets with source IP address zero
ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
        0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 info request, 0 other
        0 irdp solicitations, 0 irdp advertisements
        0 time exceeded, 0 timestamp replies, 0 info replies
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 0 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements
BGP statistics:
  Rcvd: 0 total, 0 opens, 0 notifications, 0 updates
        0 keepalives, 0 route-refresh, 0 unrecognized
  Sent: 0 total, 0 opens, 0 notifications, 0 updates
        0 keepalives, 0 route-refresh
EIGRP-IPv4 statistics:
  Rcvd: 0 total
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
PIMv2 statistics: Sent/Received
  Total: 0/0, 0 checksum errors, 0 format errors
  Registers: 0/0 (0 non-rp, 0 non-sm-group), Register Stops: 0/0,  Hellos: 0/0
  Join/Prunes: 0/0, Asserts: 0/0, grafts: 0/0
  Bootstraps: 0/0, Candidate_RP_Advertisements: 0/0
  State-Refresh: 0/0
IGMP statistics: Sent/Received
  Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
  Host Queries: 0/0, Host Reports: 0/0, Host Leaves: 0/0
  DVMRP: 0/0, PIM: 0/0
UDP statistics:
  Rcvd: 185515 total, 0 checksum errors, 185515 no port
```

```
  Sent: 0 total, 0 forwarded broadcasts
OSPF statistics:
  Rcvd: 0 total, 0 checksum errors
        0 hello, 0 database desc, 0 link state req
        0 link state updates, 0 link state acks
  Sent: 0 total
        0 hello, 0 database desc, 0 link state req
        0 link state updates, 0 link state acks
Probe statistics:
  Rcvd: 0 address requests, 0 address replies
        0 proxy name requests, 0 where-is requests, 0 other
  Sent: 0 address requests, 0 address replies (0 proxy)
        0 proxy name replies, 0 where-is replies
ARP statistics:
  Rcvd: 1477 requests, 8841 replies, 396 reverse, 0 other
  Sent: 1 requests, 20 replies (0 proxy), 0 reverse
  Drop due to input queue full: 0
```

The following is sample output from the **show ip traffic** command for Ethernet interface 0/0:

```
Router# show ip traffic interface ethernet 0/0
Ethernet0/0 IP-IF statistics :
  Rcvd:  99 total, 9900 total_bytes
         0 format errors, 0 hop count exceeded
         0 bad header, 0 no route
         0 bad destination, 0 not a router
         0 no protocol, 0 truncated
         0 forwarded
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 discards, 99 delivers
  Sent:  99 total, 9900 total_bytes 0 discards
         99 generated, 0 forwarded
         0 fragmented into, 0 fragments, 0 failed
  Mcast: 0 received, 0 received bytes
         0 sent, 0 sent bytes
  Bcast: 0 received, 0 sent
```

Examples

The following is sample output from the **show ip traffic** command when used on a Cisco 10000 series router:

```
Router# show ip traffic
IP statistics:
  Rcvd:  27 total, 27 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 27 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  0 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
         0 options denied, 0 source IP address zero
```

The table below describes the significant fields shown in the display.

Table 7: show ip traffic Field Descriptions

Field	Description
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.

Field	Description
bad hop count	Occurs when a packet is discarded because its time-to-live (TTL) field was decremented to zero.
encapsulation failed	Usually indicates that the router had no ARP request entry and therefore did not send a datagram.
no route	Counted when the Cisco IOS software discards a datagram that it did not know how to route.

Related Commands

Command	Description
clear ip traffic	Clears the global or system-wide IP traffic statistics for one or more interfaces.

show ipv6 cef with epoch

To display Cisco Express Forwarding IPv6 Forwarding Information Base (FIB) information filtered for a specific epoch, use the **show ipv6 cef with epoch** command in privileged EXEC mode.

show ipv6 cef with epoch *epoch-number* [**checksum**| **detail**| **internal [checksum]**| **platform** [**checksum**| **detail**| **internal [checksum]**]]

Syntax Description

epoch-number	Number of the epoch, from 0 to 255.
checksum	(Optional) Displays FIB entry checksums.
detail	(Optional) Displays detailed information about FIB epochs.
internal	(Optional) Displays internal data structure information.
platform	(Optional) Displays platform-specific data structures.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to display information about prefix properties for a specified epoch in the Cisco Express Forwarding IPv6 FIB. This command is similar to the **show ip cef with epoch** command, except that it is IPv6 specific. Use the **show ipv6 cef epoch**command to display entries filtered by epoch number.

Examples

The following is sample output from the **show ipv6 cef with epoch**command:

```
Router# show ipv6 cef with epoch 0
::/0
```

```
  no route
::/127
  discard
2000::1/128
  receive for Loopback0
2000::2/128
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64
  attached to Ethernet2/0
2001::1/128
  receive for Ethernet2/0
2001::3/128
  attached to Ethernet2/0
2001:1::/64
  attached to Ethernet0/0
2001:1::1/128
  receive for Ethernet0/0
2001:2::/64
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64
  attached to Tunnel0
2002::1/128
  receive for Tunnel0
FE80::/10
  receive for Null0
FF00::/8
  receive for Null0
```

The table below describes significant fields shown in the display.

Table 8: show ipv6 cef with epoch Field Descriptions

Field	Description
no route	No route is associated with the IPv6 prefix.
discard	Traffic for this prefix is discarded.
2000::1/128 receive for Loopback0	A receive prefix for interface Loopback0.
2000::2/128 nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0	An IPv6 prefix that is forwarded to a next-hop address (FE80::A8BB:CCFF:FE00:2500) through interface Ethernet 0/0.
2001::/64 attached for Ethernet2/0	This prefix is a connected network on interface Ethernet 0/0.
2001::1/128 receive for Ethernet2/0	A receive prefix for interface Ethernet 0/0.

The following is sample output from the **show ipv6 cef with epoch detail**command:

```
Router# show ipv6 cef with epoch 0 detail

IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)
```

```
::/0, epoch 0, flags default route handler
  no route
::/127, epoch 0, flags attached, discard
  discard
2000::1/128, epoch 0, flags attached, connected, receive, local
  receive for Loopback0
2000::2/128, epoch 0
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64, epoch 0, flags attached, connected, cover dependents
  Covered dependent prefixes: 1
    notify cover updated: 1
  attached to Ethernet2/0
2001::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet2/0
2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 02513FD8
   Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
2001:1::/64, epoch 0, flags attached, connected
  attached to Ethernet0/0
2001:1::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet0/0
2001:2::/64, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64, epoch 0, flags attached, connected
  attached to Tunnel0
2002::1/128, epoch 0, flags attached, receive, local
  receive for Tunnel0
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0
```

The table below describes significant fields shown in the display.

Table 9: show ipv6 cef with epoch detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally	Indicates that IPv6 CEF is enabled and running on the RP.
VRF base 16 prefixes (16/0 fwd/non-fwd)	Number of prefixes in the VRF, how many of them are forwarded, and how many are not forwarded.
Table id 0	Table identification number.
Database epoch 0 (16 entries at this epoch)	Value of the database epoch and number of entries in the epoch.

Field	Description
2000::1/128, epoch 0, flags attached, connected, receive, local receive for Loopback0	Provides detail for the table entries. In this example, 2000:1/128 is an IPv6 prefix at epoch 0. The flags set for this prefix are: • attached--Prefix is a connected network • connected--Prefix includes an address that is bound to an interface on the device • receive--Prefix is punt to and handled by the process level • local--Prefix is a subset of receive and marks prefixes that are received by on interface on the device

The following is sample output from the **show ipv6 cef with epoch checksum** command:

```
Router# show ipv6 cef with epoch 0 checksum
::/0
  FIB checksum: 0x64E25610
::/127
  FIB checksum: 0xE0B3DE11
2000::1/128
  FIB checksum: 0xD04E36EC
2000::2/128
  FIB checksum: 0x84892BA5
2000::3/128
  FIB checksum: 0x912BA720
2000::4/128
  FIB checksum: 0xC6D89ADA
.
.
.
```

The table below describes significant fields shown in the display.

Table 10: show ipv6 cef with epoch checksum Field Descriptions

Field	Description
::/0	Default route handler. ::/0 prefix matches all addresses. (::/128 prefix is an exact match for all zero addresses only.)
FIB checksum: 0x64E25610	FIB checksum associated with the named prefix.

Related Commands

Command	Description
show ip cef with epoch	Displays Cisco Express Forwarding FIB information filtered for a specific epoch.

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef epoch	Displays a summary of IPv6 FIB epoch information.

show ipv6 cef with source

To display Cisco Express Forwarding IPv6 Forwarding Information Base (FIB) filtered for a specific source, use the **show ipv6 cef with source** command in privileged EXEC mode.

show ipv6 cef with source *source-type* [**checksum**| **detail**| **epoch**| **internal [checksum]**| **platform** [**checksum**| **detail**| **internal [checksum]**]]

Syntax Description

source-type	

The *source-type*argument must be replaced by one of the following keywords that are supported for your release.

Keywords for all supported Cisco IOS releases:

- **alias** --Displays alias address prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **broadband** --Displays broadband receive prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **fallback** --Displays fallback lookup prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **interface** --Displays interface configuration prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **nat** --Displays Network Address Translation (NAT) prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **rib** --Displays Routing Information Base (RIB) prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **special** --Displays special prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **test** --Displays test command prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **virtual** --Displays virtual address prefix sources in the Cisco Express Forwarding IPv6 FIB, for example, Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP) addresses.

Additional keywords for Cisco IOS Releases 12.2(25)S, 12,2(28)SB, 12.2(33)SRA, and later SB and SR releases:

- **adjacency** --Displays adjacency prefix sources in the Cisco Express ForwardingIPv6 FIB.
- **default-route** --Displays default route handler prefix sources in the Cisco Express Forwarding FIB.
- **inherited-path-list** --Displays inherited path list prefix source in the Cisco Express Forwarding FIB.

Additional keywords for Cisco IOS Releases

	12.2(33)SXH, 12.4(20)T, and later SX and T releases: • **adj** --Displays adjacency prefix sources in the Cisco Express Forwarding FIB.
-	• **defnet--** Displays default network prefix sources in the Cisco Express Forwarding IPv6 FIB. • **defroutehandler** --Displays default route handler prefix sources in the Cisco Express Forwarding IPv6 FIB. • **ipl** --Displays inherited path list prefix source in the Cisco Express ForwardingIPv6 FIB. • **recursive-resolution** --Displays recursive resolution prefix sources in the Cisco Express Forwarding IPv6 FIB. Additional keyword for Cisco IOS Release 12.2(33)SXH and later SX releases: • **lte** --Displays Multiprotocol Label Switching (MPLS) label table entries.
checksum	(Optional) Displays IPv6 FIB entry checksums.
detail	(Optional) Displays detailed information about IPv6 FIB epochs.
epoch	(Optional) Displays information about epochs associated with the source prefix.
internal	(Optional) Displays internal data structure information.
platform	(Optional) Displays platform-specific data structures.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to filter on prefixes in the Cisco Express Forwarding FIB that are added by a specified source.

Examples

Examples

The following is sample output from the **show ipv6 cef with source rib** command:

```
Router# show ipv6 cef with source rib
::/127
  discard
2000::1/128
  receive for Loopback0
2000::2/128
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64
  attached to Ethernet2/0
2001::1/128
  receive for Ethernet2/0
2001:1::/64
  attached to Ethernet0/0
2001:1::1/128
  receive for Ethernet0/0
2001:2::/64
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64
  attached to Tunnel0
2002::1/128
  receive for Tunnel0
FE80::/10
  receive for Null0
FF00::/8
  receive for Null0
```

The table below describes the significant fields shown in the display.

Table 11: show ipv6 cef with source rib Field Descriptions

Field	Description
::/127	IPv6 prefix.
discard	Indicates that traffic destined for this prefix should be discarded.
2000::1/128 receive for Loopback0	An IPv6 prefix that is a receive prefix for interface Loopback0. Traffic destined for this prefix will be punted to the process level.

Field	Description
2000::2/128 nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0	An IPv6 prefix that is forwarded to a next-hop address (FE80::A8BB:CCFF:FE00:2500) through interface Ethernet 0/0.
2001::/64 attached for Ethernet2/0	An IPv6 prefix that is a connected network on interface Ethernet 0/0. That is, the destination can be reached directly through the specified interface.

The following is sample output from the **show ipv6 cef with source fib detail** command:

```
Router# show ipv6 cef with source rib detail
IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)
::/127, epoch 0, flags attached, discard
  discard
2000::1/128, epoch 0, flags attached, connected, receive, local
  receive for Loopback0
2000::2/128, epoch 0
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64, epoch 0, flags attached, connected, cover dependents
  Covered dependent prefixes: 1
    notify cover updated: 1
  attached to Ethernet2/0
2001::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet2/0
2001:1::/64, epoch 0, flags attached, connected
  attached to Ethernet0/0
2001:1::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet0/0
2001:2::/64, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64, epoch 0, flags attached, connected
  attached to Tunnel0
2002::1/128, epoch 0, flags attached, receive, local
  receive for Tunnel0
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0
```

The table below describes the significant fields shown in the display.

Table 12: show ipv6 cef with source rib detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled globally.
VRF base	Base VRF table.

Field	Description
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes in the VRF, how many prefixes are forwarded, and how many are not forwarded.
Table id 0	Identifies the table by number.
Database epoch:	Specifies the type of epoch.
0 (16 entries at this epoch)	Number of the epoch (0) and number of entries in the epoch.
2000::1/128, epoch 0, flags attached, connected, receive, local	Details about the prefix: the epoch in which it is found, the flags set for the prefix: • attached--Prefix is a connected network • connected--Prefix includes an address that is bound to an interface on the device • receive--Prefix is punt to and handled by the process level • local--Prefix is a subset of receive and marks prefixes that are received by on interface on the device

Examples

The following is sample output from the **show ipv6 cef with source adjacency** command:

```
Router# show ipv6 cef with source adjacency
2001::3/128
  attached to Ethernet2/0
```

The table below describes the significant fields shown in the display.

Table 13: show ipv6 cef with source adjacency Field Descriptions

Field	Description
20001::3/128	IPv6 prefix whose source is an adjacency.
attached to Ethernet2/0	Indicates that the prefix is a connected network through Interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adjacency detail**command:

```
Router# show ipv6 cef with source adjacency detail
#
IPv6 CEF is enabled and running centrally.
VRF Default
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0x1E000000
```

```
 Database epoch:        0 (16 entries at this epoch)
2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 050878F0
   Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
```

The table below describes the significant fields shown in the display.

Table 14: show ipv6 cef with source adjacency detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled and running on the RP.
VRF Default	Default VRF table.
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes in the VRF, how many prefixes are forwarded and how many are not forwarded.
Table id 0x1E000000	Identifies the table by hexadecimal number.
2001::3/128, epoch 0, flags attached	Lists a prefix, its epoch number, and flags. Attached flag indicates a connected network.
Adj source: IPv6 adj out of Ethernet2/0, addr 2000::3 050878F0	Indicates that the prefix was sourced by an adjacency and specifies the address family, interface, and address in memory of the adjacency.
Dependent covered prefix type adjfib cover 2001::/64	A prefix sourced by an adjacency is dependent on another less specific prefix (2001::/64) for forwarding information. If this less specific prefix changes, the dependent prefix will need to be recomputed.
attached to Ethernet2/0	Indicates the prefix is a connect network through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adjacency checksum**command:

```
Router# show ipv6 cef with source adjacency checksum
2001::3/128
  FIB checksum: 0x4AE0F5DC
```

The table below describes the significant fields shown in the display.

Table 15: show ipv6 cef with source adjacency checksum Field Descriptions

Field	Description
2001::3/128	IPv6 prefix whose source is an adjacency.
FIB checksum: 0x4AE0F5DC	FIB checksum.

Examples

The following is sample output from the **show ipv6 cef with source adjacency** command:

```
Router# show ipv6 cef with source adj
2001::3/128
  attached to Ethernet2/0
```

The table below describes the significant fields shown in the display.

Table 16: show ipv6 cef with source adj Field Descriptions

Field	Description
20001::3/128	IPv6 prefix whose source is an adjacency.
attached to Ethernet2/0	Indicates that the prefix is a network connected through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adj detail**command:

```
Router# show ipv6 cef with source adj detail
IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)
2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 02513FD8
   Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
```

The table below describes the significant fields shown in the display.

Table 17: show ipv6 cef with source adj detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled an running on the RP.
VRF base	Base VRF table.
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes, and how many prefixes are forwarded and how many are not forwarded.
2001::3/128, epoch 0, flags attached	Provides more detail about the adjacency source, such as epoch number and flags.
Adj source: IPv6 adj out of Ethernet2/0, addr 2000::3 050878F0	Lists a prefix, its epoch number, and flags. Attached flag indicates a connected network.
Dependent covered prefix type adjfib cover 2001::/64	A prefix sourced by an adjacency is dependent on another less specific prefix (2001::/64) for forwarding information. If this less specific prefix changes, the dependent prefix will need to be recomputed.

Field	Description
attached to Ethernet2/0	Indicates the prefix is a connect network through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adj checksum**command:

```
Router# show ipv6 cef with source adj checksum
2001::3/128
  FIB checksum: 0x4AE0F5DC
```

The table below describes the significant fields shown in the display.

Table 18: show ipv6 cef with source adj checksum Field Descriptions

Field	Description
2001::3/128	IPv6 prefix whose source is an adjacency.
FIB checksum: 0x4AE0F5DC	FIB checksum.

Related Commands

Command	Description
show ip cef	Displays entries in the FIB or displays a summary of the FIB.
show ip cef with epoch	Displays information about an epoch in the Cisco Express Forwarding FIB.
show ipv6 cef with epoch	Displays information about an epoch in the Cisco Express Forwarding IPv6 FIB.
show ipv6 cef with source	Displays information about prefix sources in the Cisco Express Forwarding IPv6 FIB.

show mls cef

To display the Multilayer Switching (MLS)-hardware Layer 3-switching table entries, use the **show mls cef** command in user EXEC and privileged EXEC mode.

show mls cef [ip] [*prefix* [*mask-length*| **load-info**]] **[detail]** [**module** *number*]

show mls cef [ip] [**lookup** ...| **multicast** ...| **rpf** ...| **vpn** ...| **vrf** ...]

show mls cef [**adjacency** ...| **block** *block-number* **[entries]**| **config-register** *reg-address*| **diags [detail]**| **entry** *index* **[detail]**| **exact-route** ...| **hardware** [**module** *number*]| **inconsistency** ...| **lookup** ...| **masks** [*type*] [**module** *number*]| **rpf** ...| **statistics** ...| **summary** [**module** *number*]| **tunnel fragment**| **used-blocks** [*type*] [**module** *number*]| **vpn** ...| **vrf** ...]

show mls cef [**eom** ...| **ip** ...| **ipv6** ...| **mpls** ...]

Syntax Description

ip	(Optional) Displays IPv6 unicast entries in the MLS-hardware Layer 3-switching table; see the "Usage Guidelines" section for additional information.
prefix	(Optional) Entry prefix in the format A.B.C.D.
mask-length	(Optional) Mask length; valid values are from 0 to 32.
load-info	(Optional) Displays output with a hash value next to each adjacency.
detail	(Optional) Displays detailed hardware information. See the "Usage Guidelines" section for important information.
module *number*	(Optional) Displays information about the entries for a specific module.
lookup ...	(Optional) Displays IP entries in the MLS-hardware Layer 3-switching table for the specified destination IP address. See the **show mls cef lookup** command.
multicast ...	(Optional) Displays IP entries in the MLS-hardware Layer 3-switching table in the compact Cisco Express Forwarding table display format; see the **show mls cef ip multicast** command.
rpf ...	(Optional) Displays information about the Reverse Path Forwarding (RPF) hardware in the MLS-hardware Layer 3-switching table; see the **show mls cef rpf** command.

vpn ...	(Optional) Displays information about the Virtual Private Network (VPN) ID Cisco Express Forwarding table. See the "Usage Guidelines" section for important information.
vrf ...	(Optional) Displays information about the Cisco Express Forwarding table for the specified VRF name.
adjacency ...	(Optional) Displays information about the MLS-hardware Layer 3-switching adjacency node; see the **show mls cef adjacency** command.
block *block-number*	(Optional) Displays information about the mask-block utilization for a specific block; valid values are from 0 to 4294967295. See the "Usage Guidelines" section for important information.
entries	(Optional) Displays the mask-block utilization entries. See the "Usage Guidelines" section for important information.
config-register *reg-address*	(Optional) Displays information about the hardware configuration register for a specific register. See the "Usage Guidelines" section for important information.
diags	(Optional) Displays information about the diagnostic entry. See the "Usage Guidelines" section for important information.
entry *index*	(Optional) Specifies the specified prefix entry index to display; valid values are from 0 to 4294967295. See the "Usage Guidelines" section for important information.
exact-route ...	(Optional) Displays information about hardware load sharing; see the **show mls cef exact-route** command.
hardware	(Optional) Displays a summary of the hardware information. See the "Usage Guidelines" section for important information.
inconsistency ...	(Optional) Displays information about the consistency checker; see the **show mls cef inconsistency** command.
masks ...	(Optional) Displays information about the mask. See the "Usage Guidelines" section for important information.

statistics ...	(Optional) Displays the number of switched packets and bytes; see the **show mls cef statistics** command.
tunnel fragment	(Optional) Displays the operational status of tunnel fragmentation.
summary ...	(Optional) Displays a summary of rates in the hardware for each protocol; see the **show mls cef summary** command.
used-blocks	(Optional) Displays a list of used blocks; see the "Usage Guidelines" section for important information.
eom ...	Displays information about the EoM protocol; this keyword is not supported.
ip ...	Displays information about the IP protocol; see the "Usage Guidelines" section for additional information.
ipv6 ...	Displays information about the IPv6 protocol.
mpls ...	Displays information about the MPLS protocol; see the **show mls cef mpls** command.

Command Default

If you do not specify a protocol, the default display is for IP and the global Cisco Express Forwarding table.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to support the **mpls** keyword.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2SX release. This command was changed to include the **load-info** keyword on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(18)SXF	This command was modified. This command was changed to support the **tunnel fragment** keywords in all PFC3 modes.
12.2(33)SXH	This command was modified. Support for the command was added for PCF3BXL, PFC3C, and PFC3CXL modes only.
12.2(33)SXI	This command was modified. Support for the command was added for PCF3BXL, PFC3C, and PFC3CXL modes only.

Release	Modification
12.2(33)SXI2	This command was modified. Support was added for all PFC3 modes.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **...** indicates that there is additional information.

The following options are for expert users only and are not documented:

- **load-info**
- **detail**
- **block** *block-number* [**entries**]
- **config-register** *reg-address* }
- **diags** [**detail**]
- **entry** *index* [**detail**]
- **hardware** [**module** *number*]
- **masks** [*type*]
- **used-blocks** [*type*]
- **vpn**

The MLS-hardware Layer 3 switching applies to IP traffic only.

Use the **show mls cef**[**ip**] **vrf** command to display the VRF Cisco Express Forwarding table entries.

You can enter this command on the supervisor engine or switch consoles. Enter the **remote login** command to session into the supervisor engine to enter the commands.

The **show mls cef** command offers three levels of options as follows:

- Protocol-independent options--The following keywords are not protocol specific:
  - **adjacency**
  - **exact-route**
  - **inconsistency**
  - **module**
  - **rpf**
  - **statistics**
  - **summary**
  - **used-blocks**
  - **vpn**
  - **vrf**

- Protocol-dependent keywords--The following keywords specify a protocol:
  - **eom**
  - **ip**
  - **ipv6**
  - **mpls**
- Default keywords--The following keywords display identical output for both the **show mls cef** and **show mls cef ip** commands:
  - *prefix*
  - **lookup**
  - **multicast**--This keyword is not supported on systems configured with a Supervisor Engine 720.
  - **module**
  - **rpf**
  - **vpn**
  - **vrf**

Examples

This example shows how the **show mls cef** and **show mls cef ip** commands are identical:

```
Router#
show mls cef
Codes: decap - Decapsulation, + - Push Label
Index  Prefix              Adjacency
66     127.0.0.1/32         punt
67     10.1.1.100/32        punt
68     10.1.1.0/32          punt
69     10.1.1.255/32        punt
70     10.2.2.100/32        punt
71     10.2.2.0/32          punt
72     10.2.2.255/32        punt
73     10.2.2.5/32          Gi5/2,          0000.c005.0205
74     0.0.0.0/32           punt
75     10.255.255.255/32    punt
76     172.16.22.22/32      punt
77     172.20.0.0/32        punt
78     173.32.255.255/32    punt
79     172.16.1.153/32      Vl30,           0050.808b.8200
81     172.16.1.91/32       Vl30,           0004.4eef.8800
82     172.16.1.100/32      Vl30,           00d0.bb02.0400
83     172.17.223.3/32      Vl30,           00d0.061b.7000
84     172.22.5.3/32        Vl30,           00d0.061d.200a
85     172.16.1.101/32      Vl30,           0007.ecfc.e40a
86     172.20.100.1/32      Vl30,           0050.2a8d.700a
87     172.16.1.104/32      Vl30,           0050.0f2d.ac00
88     172.32.254.226/32    Vl30,           0050.2a8d.700a
89     10.2.2.7/32          Gi5/2,          0000.c005.0207
90     10.1.1.5/32          Gi5/1,          0000.0101.0105
3200   224.0.0.0/8          punt
3201   10.1.1.0/24          punt
3202   10.2.2.0/24          punt
134400 172,20.0.0/8         punt
134432 0.0.0.0/0            drop
524256 0.0.0.0/0            drop
Router#
```

This example shows how to display all the MLS-hardware Layer 3-switching table IP entries:

```
Router#
show mls cef ip
Codes: decap - Decapsulation, + - Push Label
Index  Prefix              Adjacency
66     127.0.0.1/32         punt
67     10.1.1.100/32        punt
68     10.1.1.0/32          punt
69     10.1.1.255/32        punt
70     10.2.2.100/32        punt
71     10.2.2.0/32          punt
72     10.2.2.255/32        punt
73     10.2.2.5/32          Gi5/2,          0000.c005.0205
74     0.0.0.0/32           punt
75     10.255.255.255/32    punt
76     172.16.22.22/32      punt
77     172.20.0.0/32        punt
78     173.32.255.255/32    punt
79     172.16.1.153/32      Vl30,           0050.808b.8200
81     172.16.1.91/32       Vl30,           0004.4eef.8800
82     172.16.1.100/32      Vl30,           00d0.bb02.0400
83     172.17.223.3/32      Vl30,           00d0.061b.7000
84     172.22.5.3/32        Vl30,           00d0.061d.200a
85     172.16.1.101/32      Vl30,           0007.ecfc.e40a
86     172.20.100.1/32      Vl30,           0050.2a8d.700a
87     172.16.1.104/32      Vl30,           0050.0f2d.ac00
88     172.32.254.226/32    Vl30,           0050.2a8d.700a
89     10.2.2.7/32          Gi5/2,          0000.c005.0207
90     10.1.1.5/32          Gi5/1,          0000.0101.0105
3200   224.0.0.0/8          punt
3201   10.1.1.0/24          punt
3202   10.2.2.0/24          punt
134400 172,20.0.0/8         punt
134432 0.0.0.0/0            drop
524256 0.0.0.0/0            drop
Router#
```

The table below describes the fields in the examples.

Table 19: show mls cef Command Output Fields

Field	Description
Index	MLS-hardware Layer 3-switching table entry index; the maximum is 256,000 entries.
Prefix	Entry prefix address/mask.
Adjacency	Adjacency types are as follows: • drop--Packets matching the prefix entry are dropped. • punt--Packets are redirected to an MSFC for further processing. • **mac-address** --Packets matching the prefix are forwarded to this specific next hop or the final destination host if directly attached.

This example shows how to display the operational status of tunnel fragmentation:

```
Router# show mls cef tunnel fragment
Tunnel Fragmentation:       Enabled
Router#
```

Related Commands

Command	Description
show mls cef summary	Displays the number of routes in the MLS-hardware Layer 3-switching table for all the protocols.

show mls cef adjacency

To display information about the Multilayer Switching (MLS)-hardware Layer 3-switching adjacency node, use the **show mls cef adjacency** command in user EXEC or privileged EXEC mode.

show mls cef adjacency [**all**| **decap-tunnel**| **encap-tunnel** *ip-src-addr*| **entry** *index* [**to** *end-range*]| **flags** *lower-flag upper-flag*| **mac-address** *number*| **mac-rewrite**| **macv4**| **mpls** [*label*]| **multicast**| **nat**| **recirculation**| **special**| **tcp**| **usage**] **[detail]** [**module** *number*]

Syntax Description

all	(Optional) Displays all application-allocated entries.
decap-tunnel	(Optional) Displays the decapsulated tunneled-packet information.
encap-tunnel *ip-src-addr*	(Optional) Displays the encapsulated tunnel-adjacency entry that matches the specified address.
entry *index*	(Optional) Displays the adjacency-entry information for the specified index; valid values are from 0 to 1048575.
to *end-range*	(Optional) Specifies the index range to display adjacency-entry information; valid values are from 0 to 1048575.
flags	(Optional) Displays information about the specified bit flags. See the "Usage Guidelines" section for additional information.
lower-flag	Lower 32-bits flag values to display; valid values are 0 to FFFFFFFF.
upper-flag	Upper 32-bits flag values to display; valid values are 0 to FFFFFFFF.
mac-address *number*	(Optional) Displays information about the matched MAC-address adjacency for the specified 48-bit hardware address in the H.H.H format.
mac-rewrite	(Optional) Displays information about the MAC-rewrite adjacency.
macv4	(Optional) Displays information about the MACv4 adjacency.
mpls	(Optional) Displays information about the Multiprotocol Label Switching (MPLS) adjacency.

label	(Optional) MPLS label to display adjacency-entry information; valid values are from 0 to 1048575.
multicast	(Optional) Displays information about the multicast adjacency.
nat	(Optional) Displays information about the Network Address Translation (NAT) adjacency.
recirculation	(Optional) Displays information about the recirculated-adjacency entry.
special	(Optional) Displays information about the special adjacencies.
tcp	(Optional) Displays information about the TCP-application adjacency.
usage	(Optional) Displays information about the adjacency usage.
detail	(Optional) Displays hardware-entry details.
module *number*	(Optional) Displays information about the adjacency node for a specific module.

Command Modes

User EXEC (>) Privileged EXEC (#)

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 the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **decap-tunnel** and **endcap-tunnel** keywords are used to display the tunnel nodes. The encapsulator node is considered the tunnel-entry point and the decapsulator node is considered the tunnel-exit point. There may be multiple source-destination pairs using the same tunnel between the encapsulator and decapsulator.

The **decap-tunnel** and **endcap-tunnel**keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The **flags** keyword applies to all adjacency formats (for example, mac-rewrite, mpls, and multicast) and indicates the bits that are set in the adjacency for the specific adjacency.

The **module** *number* keyword and argument designate the module and port number. Valid values depend on the chassis and module used. For example, if you have a 48-port 10/100BASE-T Ethernet module 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.

MLS-hardware Layer 3 switching applies to IP traffic only.

MLS-hardware Layer 3-switching adjacency statistics are updated every 60 seconds.

You can display hardware-switched IP-directed broadcast information by entering the **show mls cef adjacency mac-address** *number* **detail** command.

For each MLS-hardware Layer 3-switching Forwarding Information Base (FIB) entry, MLS-hardware Layer 3 switching stores Layer 2 information from the MSFC2 for adjacent nodes in the MLS-hardware Layer 3-switching adjacency table. Adjacent nodes are directly connected at Layer 2. To forward traffic, MLS-hardware Layer 3 switching selects a route from a MLS-hardware Layer 3-switching FIB entry, which points to a MLS-hardware Layer 3-switching adjacency entry, and uses the Layer 2 header for the adjacent node in the adjacency table entry to rewrite the packet during Layer 3 switching. MLS-hardware Layer 3 switching supports one million adjacency-table entries.

Examples

Examples

These examples show the output from Cisco 7600 series routers that are configured with a Supervisor Engine 720.

This example shows how to display information for all adjacency nodes:

```
Router# show mls cef adjacency all
Index: 5       smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
               packets: 0, bytes: 0
Index: 32773   smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
               packets: 0, bytes: 0
<Output is truncated>
```

This example shows how to display the adjacency-entry information for a specific index:

```
Router# show mls cef adjacency entry 132
Index: 132     smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
               packets: 0, bytes: 0
```

This example shows how to display the adjacency-entry information for a range of indexes:

```
Router# show mls cef adjacency entry 132 to 134
Index: 132     smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
               packets: 0, bytes: 0
Index: 133     smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
               packets: 0, bytes: 0
Index: 134     smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
               packets: 0, bytes: 0
Router#
```

This example shows how to display recirculation-adjacency information:

```
Router# show mls cef adjacency recirculation detail
Index: 6       smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 65535, vlan: 0, dindex: 0x0, ccc = 110,
               format: RECIR, l3rw_vld: 1
Router#
```

This example shows how to display specific bit flags:

```
Router# show mls cef adjacency flags 8408 0

STAT_REQUIRED NO_STAT CAP1 IQO UTTL UTOS
Router#
```

This example shows how to display adjacency-node information for a specific MAC address:

```
Router# show mls cef adjacency mac-address 00e0.f74c.842d
Index: 133138  smac: 00d0.061d.200a, dmac: 00e0.f74c.842d
               mtu: 1518, vlan: 45, dindex: 0x0, l3rw_vld: 1
               packets: 0, bytes: 0
Index: 133144  smac: 00d0.061d.200a, dmac: 00e0.f74c.842d
               mtu: 1518, vlan: 45, dindex: 0x0, l3rw_vld: 1
               packets: 0, bytes: 0
Router#
```

This example shows how to display the MAC-rewrite adjacency information:

```
Router# show mls cef adjacency mac-rewrite
Index: 133132  smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
               packets: 0, bytes: 0
Index: 133133  smac: 000a.421f.3000, dmac: 0050.2a8d.700a
               mtu: 1518, vlan: 1, dindex: 0x0, l3rw_vld: 1
               packets: 0, bytes: 0
Index: 133134  smac: 000a.421f.3000, dmac: 0000.7201.0001
               mtu: 1518, vlan: 72, dindex: 0x0, l3rw_vld: 1
               packets: 0, bytes: 0
Index: 133135  smac: 000a.421f.3000, dmac: 0000.7301.0001
               mtu: 1518, vlan: 73, dindex: 0x0, l3rw_vld: 1
               packets: 0, bytes: 0
<Output is truncated>
```

This example shows how to display information about the MPLS adjacency:

```
Router#  show mls cef adjacency mpls detail
Index: 32768 smac: 0000.0000.0000, dmac: 0000.0000.0000
mtu: 1514, vlan: 0, dindex: 0x7FFA, l3rw_vld: 1
format: MPLS, flags: 0x1000408600
label0: 0, exp: 0, ovr: 0
label1: 0, exp: 0, ovr: 0
label2: 0, exp: 0, ovr: 0
op: POP
packets: 0, bytes: 0
Router#
```

This example shows how to display information about the multicast adjacency:

```
Router# show mls cef adjacency
 multicast detail
Index: 22 smac: 0000.0000.0000, dmac: 0000.0000.0000
mtu: 0, vlan: 0, dindex: 0x0, l3rw_vld: 0
format: MULTICAST, flags: 0x800
met2: 0, met3: 0
packets: 2232, bytes: 180684
Router#
```

This example shows how to display information about the NAT adjacency:

```
Router# show mls cef adjacency
 nat detail
Index: 200 mtu: 1522, vlan: 1063, dindex: 0x7FFA, l3rw_vld: 1
format: NAT, flags: 0x8600
ip_sa: 10.2.2.2, src_port: 100
ip_da: 10.3.3.3, dst_port: 300
delta_seq: 0, delta_ack: 0
packets: 0, bytes: 0
Router#
```

This example shows how to display information about the special adjacency:

```
Router# show mls cef adjacency special
Index: 0       smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 0
               format: MULTICAST, flags: 0x800 (mcast_fib_fail)
               met2: 0, met3: 0
               packets: 0, bytes: 0
Index: 1       smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 0
               format: MULTICAST, flags: 0x800 (mcast_fib_rf_cr)
               met2: 0, met3: 0
               packets: 0, bytes: 0
<Output is truncated>
```

This example shows how to display information about the TCP adjacency:

```
Router# show mls cef adjacency tcp detail
Index: 200 smac: abcd.abcd.abcd, dmac: 0000.1000.2000
mtu: 1518, vlan: 1063, dindex: 0x0, l3rw_vld: 1
format: MAC_TCP, flags: 0x8408
delta_seq: 10, delta_ack: 0
packets: 0, bytes: 0
Router#
```

This example shows how to display information about the adjacency usage:

```
Router# show mls cef adjacency usage
Adjacency Table Size: 1048576
ACL region usage: 2
Non-stats region usage: 128
Stats region usage: 31
Total adjacency usage: 161
Router#
```

Examples

These examples show the output from Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This example shows how to display information for all adjacency nodes:

```
Router# show mls cef adjacency
Index 17414 : mac-sa:00d0.061d.200a, mac-da:0000.0000.0b0b
               interface:Gi4/11, mtu:1514
               packets:0000000000000000, bytes:0000000000000000
Index 17415 : mac-sa:00d0.061d.200a, mac-da:00e0.f74c.842e
               interface:Vl46, mtu:1514
               packets:0000000000000000, bytes:0000000000000000
Router#
```

This example shows how to display adjacency-node information for a specific MAC address:

```
Router# show mls cef adjacency mac-address 00e0.f74c.842e
Index 17415 : mac-sa:00d0.061d.200a, mac-da:00e0.f74c.842e
              interface:Vl46, mtu:1514
              packets:0000000000000000, bytes:0000000000000000
Router#
```

This example shows how to display the adjacency node information for a specific MAC address for a specific module:

```
Router# show mls cef adjacency mac-address 00e0.f74c.842e module 4
Module 4#
Index 17415 : mac-sa:00d0.061d.200a, mac-da:00e0.f74c.842e
              interface:Vl46, mtu:1514
              packets:0000000000000000, bytes:0000000000000000
Router#
```

show mls cef exact-route

To display information about the hardware load sharing, use the **show mls cef exact-route** command in user EXEC or privileged EXEC mode.

show mls cef exact-route {**vrf** *instance-name src-ip*| *src-ip*} {*dest-ip*| *src-l4port*} [*dest-l4port*| **module** *num*]

Syntax Description

vrf *instance-name*	Displays the numeric Virtual Private Network (VPN) routing and forwarding (VRF) ID for the specified VRF instance name.
src-ip	Source IP address.
dest-ip	Destination IP address.
src-l4port	Layer 4-source port number; valid values are from 0 to 65535.
dest-l4port	(Optional) Layer 4-destination port number; valid values are from 0 to 65535.
module *num*	(Optional) Module number.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to include the **vrf** *instance-name*keyword and argument.
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.

Usage Guidelines

The **vrf** *i nstance-name* keyword and argument are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the hardware load-sharing information. The fields shown in the display are self-explanatory.

```
Router# show mls cef exact-route 172.20.52.16 172.20.52.31
Interface: Gi2/1, Next Hop: 255.255.255.255, Vlan: 4073, Destination Mac: 00d0.061d.200a
Router#
```

Related Commands

Command	Description
show ip cef exact-route	Displays the exact route for a source-destination IP address pair.

show mls cef exception

To display information about the Cisco Express Forwarding exception, use the **show mls cef exception** command in user EXEC or privileged EXEC mode.

Note The **show mls cef exception** command is not available in Cisco IOS Release 12.2(33)SXJ and later Cisco IOS 12.2SX releases.

show mls cef exception {**status [detail]**| **priorities**}

Syntax Description

status	Displays information about the Cisco Express Forwarding exception status.
detail	(Optional) Displays detailed hardware information; see the "Usage Guidelines" section for more information.
priorities	Displays information about the Cisco Express Forwarding exception priority.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX1	The output was changed to display IPv6 information.
12.2(17b)SXA	The output was changed to display Multiprotocol Label Switching (MPLS) information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXJ	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXJ and later Cisco IOS 12.2SX releases.

Usage Guidelines

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

The **detail** keyword is for expert users only and is not documented.

In the output of the **show mls cef exception status** command, the following definitions apply:

- FALSE--Indicates that the protocol is not under the exception.
- TRUE--Indicates that the protocol is under the exception.

Examples

This example shows how to display detailed information about the Cisco Express Forwarding exception status. The fields shown in the display are self-explanatory.

```
Router
# show mls cef exception status
Current IPv4 FIB exception state = FALSE
Current IPv6 FIB exception state = FALSE
Current MPLS FIB exception state = FALSE
Router
#
```

This example shows how to display the Forwarding Information Base (FIB) Error Rate Monitor (ERM) exception priority. The fields shown in the display are self-explanatory.

```
Router
# show mls cef exception priorities
Priority Protocol
=====================
1 IPv4
2 IPv6
3 MPLS
Router
#
```

Related Commands

Command	Description
mls erm priority	Assigns the priorities to define an order in which protocols attempt to recover from the exception status.

show mls cef hardware

To display the Multilayer Switching (MLS)-hardware Layer 3-switching table entries, use the **show mls cef hardware** command in user EXEC or privileged EXEC mode.

show mls cef hardware [**module** *number*]

Syntax Description

module *number*	(Optional) Displays the adjacency-node information for a specific module.

Command Modes

User EXEC (>) Privileged EXEC (#)

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 the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In Cisco 7600 series routers that are configured with a Supervisor Engine 2 with a Policy Feature Card (PFC) and an Multilayer Switching Feature Card 2 (MSFC2), MLS-hardware Layer 3 switching provides IP unicast and IP multicast Layer 3 switching for a Supervisor Engine 2, a PFC2, an MSFC2, and fabric-enabled switching modules that have a Distributed Feature Card (DFC).

MLS-hardware Layer 3 switching applies to IP traffic only.

Examples

Examples

This example shows the output from Cisco 7600 series routers that are configured with a Supervisor Engine 720.

This example shows how to display all the MLS-hardware Layer 3-switching table entries:

```
Router# show mls cef hardware
  CEF TCAM v2:
  Size:
        65536 rows/device, 2 device(s), 131072 total rows
        32 entries/mask-block
        8192 total blocks (32b wide)
        0 - 4095 upper blocks, 4096 - 8191 lower blocks
        1179648 s/w table memory
  Used blocks:
        Upper bank:
          63 IP ucast
```

```
          0 IPX
          0 IP mcast
        Lower bank:
          0 IP ucast
          0 IPX
          0 IP mcast
  Free blocks (non-contiguous range):
        27 - 4095 upper blocks, 4096 - 8191 lower blocks
  Options:
        sanity check: off
        sanity interval: 301 seconds
        consistency check: on
            consistency check interval: 61 seconds
        redistribution: off
            redistribution interval: 120 seconds
            redistribution threshold: 10
        compression: on
            compression interval: 30 seconds
        bank balancing: off
            bank differential limit: 5
        rpf mode: off
        tcam shadowing: on
  Background Task statistics:
        sanity check count: 0000000000000169
        Consistency check count: 0000000000000834
        Consistency check errors: 0000000000000002
        block redistribute count:   0000000000000000
        block compress count:       0000000000000011
               IP ucast [29]:       0000000000000001
               IP ucast [28]:       0000000000000001
  Hardware switching status:
        ip switching:  on
        ipx switching: off
Router#
```

Examples

This example shows the output from Cisco 7600 series routers that are configured with a Supervisor Engine 720.

This example shows how to display all the MLS-hardware Layer 3-switching table entries:

```
Router# show mls cef hardware
 CEF TCAM v2:
  Size:
        65536 rows/device, 4 device(s), 262144 total rows
        32 entries/mask-block
        8192 total blocks (32b wide)
        1212416 s/w table memory
  Options:
        sanity check: on
        sanity interval: 301 seconds
        consistency check: on
        consistency interval: 61 seconds
        redistribution: off
            redistribution interval: 120 seconds
            redistribution threshold: 10
        compression: on
            compression interval: 31 seconds
        tcam/ssram shadowing: on
  Operation Statistics:
        Entries inserted:               0000000000000024
        Entries deleted:                0000000000000005
        Entries compressed:             0000000000000000
        Blocks inserted:                0000000000000018
        Blocks deleted:                 0000000000000004
        Blocks compressed:              0000000000000000
        Blocks shuffled:                0000000000000002
        Blocks deleted for exception:   0000000000000000
        Direct h/w modifications:       0000000000000000
  Background Task Statistics:
        Consistency Check count:        0000000000014066
```

```
        Consistency Errors:             0000000000000000
        SSRAM Consistency Errors:       0000000000000000
        Sanity Check count:             0000000000002855
        Sanity Check Errors:            0000000000000000
        Compression count:              0000000000004621
        Exception Handling status    : on
        L3 Hardware switching status : on
        Fatal Error Handling Status  : Reset
        Fatal Errors:                   0000000000000000
        Fatal Error Recovery Count:     0000000000000000
  SSRAM ECC error summary:
        Uncorrectable ecc entries    : 0
        Correctable ecc entries      : 0
        Packets dropped              : 0
        Packets software switched    : 0
FIB SSRAM Entry status
----------------------
Key: UC - Uncorrectable error, C - Correctable error
        SSRAM banks  :  Bank0    Bank1
No ECC errors reported in FIB SSRAM.
```

show mls cef inconsistency

To display consistency-checker information, use the **show mls cef inconsistency** command in user EXEC or privileged EXEC mode.

show mls cef inconsistency [**module** *num*| **now**| **records**] **[detail]** [**module** *num*]

Syntax Description

module *num*	(Optional) Displays inconsistency information for the specified module.
now	(Optional) Runs a consistency check and displays any issues.
records	(Optional) Displays the inconsistency records.
detail	(Optional) Displays hardware-entry details.
module *num*	(Optional) Displays the adjacency-node information for a specific module.

Command Modes

User EXEC (>) Privileged EXEC (#)

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 was implemented on the Supervisor Engine 2 for Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

If you enter the **show mls cef inconsistency** command with no arguments, this information is displayed:

- Consistency check count
- Ternary Content Addressable Memory (TCAM)-consistency check errors
- Synchronous static random access memory (SSRAM)-consistency check errors

Examples

This sections contains examples from the **show mls cef inconsistency**command. The fields shown in the displays are self-explanatory.

This example shows how to display information about the consistency checker:

```
Router# show mls cef inconsistency
Consistency Check Count       : 81
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
Router#
```

This example shows how to display information about the consistency checker for a specific module:

```
Router# show mls cef inconsistency module 7
Consistency Check Count       : 11033
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
Router#
```

This example shows how to run a consistency check and display any issues:

```
Router#  show mls cef inconsistency now
Performing TCAM check now ...done
No. of FIB TCAM Consistency Check Errors  : 0
Performing SSRAM check now ...done
No. of FIB SSRAM Consistency Check Errors : 0
Router#
```

This example shows how to display the consistency records:

```
Router# show mls cef inconsistency records
Consistency Check Count       : 11044
TCAM Consistency Check Errors : 0
SSRAM Consistency Check Errors : 0
Router#
```

show mls cef ip

To display the IP entries in the Multilayer Switching (MLS)-hardware Layer 3-switching table, use the **show mls cef ip** command in user EXEC or privileged EXEC mode.

show mls cef ip [*prefix* [*mask-length*]] **[detail]** [**module** *number*]

show mls cef ip accounting per-prefix

show mls cef ip {{**lookup ...**}| {**multicast tcam ...**}| {**rpf ...**}| {**vpn ...**}| {**vrf ...**}}

Syntax Description

prefix	(Optional) Entry prefix in the format A.B.C.D.
mask-length	(Optional) Mask length; valid values are from 0 to 32.
detail	(Optional) Displays hardware-entry details.
module *number*	(Optional) Displays the entries for a specific module.
accounting per-prefix	Displays all the prefixes that are configured for the statistic collection.
lookup ...	Displays the Ternary Content Addressable Memory (TCAM)-entry index for the specified destination IP unicast address; see the **show mls cef lookup** command.
multicast tcam ...	Displays the IP entries in the MLS-hardware Layer 3-switching table in the compact Cisco Express Forwarding table-display format; see the "Usage Guidelines" section for additional information.
rpf ...	Displays the Reverse Path Forwarding (RPF)--hardware information in the MLS-hardware Layer 3-switching table; see the **show mls cef rpf** command.
vpn ...	(Optional) Displays information about the Virtual Private Network (VPN) ID Cisco Express Forwarding table; see the "Usage Guidelines" section for more information.
vrf ...	Displays information about the VPN-instance Cisco Express Forwarding table.

Command Modes User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to include the **rpf** *prefix* form of this command.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

For Cisco 7600 series routers that are configured with a Supervisor Engine 720, see the **show mls cef ip multicast tcam** command for information about this command.

For Cisco 7600 series routers that are configured with a Supervisor Engine 2, the supported syntax for the **show mls cef ip multicast tcam** command is **show mls cef ip** {**multicast tcam**[*prefix* [*mask*]} [**module** *num*]].

The following keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2:

- **detail**
- **rpf**
- **vpn**
- **vrf**

The **...** indicates that there is additional information.

The **vpn** keyword is for expert users only and is not documented.

Information in the output of the **show mls cef ip** command is also displayed in the **show mls cef** commands.

The lookup is performed as a "longest prefix match" and displays the TCAM-entry index that applies to the specified destination IP address.

The information output is in this format: Index, Prefix, Mask, and Adjacency.

Examples

Supervisor Engine 2 **Examples**

These examples show the output from Cisco 7600 series routers that are configured with a Supervisor Engine 720.

This example shows how to display IP entries in the MLS-hardware Layer 3-switching table:

```
Router# show mls cef ip
Index      Prefix          Mask              Adjacency
```

```
0          0.0.0.0          255.255.255.255     punt
1          255.255.255.255  255.255.255.255     punt
2          127.0.0.12       255.255.255.255     punt
3          127.0.0.0        255.255.255.255     punt
4          127.255.255.255  255.255.255.255     punt
5          172.20.52.18     255.255.255.255     punt
6          172.20.52.0      255.255.255.255     punt
7          172.20.52.31     255.255.255.255     punt
8          172.20.52.1      255.255.255.255     0010.0d59.b8c0
160        172.20.52.0      255.255.255.224     punt
6400       224.0.0.0        255.255.255.0       punt
115200     0.0.0.0          0.0.0.0             0010.0d59.b8c0
```

This example shows how to display the longest-prefix match lookup:

```
Router# show mls cef ip lookup 172.20.52.19
160        172.20.52.0      255.255.255.224     punt
```

Supervisor Engine 720 **Examples**

These examples show the output from Cisco 7600 series routers that are configured with a Supervisor Engine 720.

This example shows how the **show mls cef** and **show mls cef ip** commands are identical:

```
Router#
show mls cef
Codes: decap - Decapsulation, + - Push Label
Index  Prefix              Adjacency
64     127.0.0.51/32       punt
65     127.0.0.0/32        punt
66     127.255.255.255/32  punt
67     1.1.1.100/32        punt
68     1.1.1.0/32          punt
69     1.1.1.255/32        punt
70     2.2.2.100/32        punt
71     2.2.2.0/32          punt
72     2.2.2.255/32        punt
73     2.2.2.5/32          Gi5/2,          0000.c005.0205
74     0.0.0.0/32          punt
75     255.255.255.255/32  punt
76     200.1.22.22/32      punt
77     200.0.0.0/32        punt
78     200.255.255.255/32  punt
79     200.1.1.153/32      Vl30,           0050.808b.8200
81     200.1.1.91/32       Vl30,           0004.4eef.8800
82     200.1.1.100/32      Vl30,           00d0.bb02.0400
83     200.12.223.3/32     Vl30,           00d0.061b.7000
84     200.2.5.3/32        Vl30,           00d0.061d.200a
85     200.1.1.101/32      Vl30,           0007.ecfc.e40a
86     200.0.100.1/32      Vl30,           0050.2a8d.700a
87     200.1.1.104/32      Vl30,           0050.0f2d.ac00
88     223.255.254.226/32  Vl30,           0050.2a8d.700a
89     2.2.2.7/32          Gi5/2,          0000.c005.0207
90     1.1.1.5/32          Gi5/1,          0000.0101.0105
3200   224.0.0.0/24        punt
3201   1.1.1.0/24          punt
3202   2.2.2.0/24          punt
134400 200.0.0.0/8         punt
134432 0.0.0.0/0           drop
524256 0.0.0.0/0           drop
Router#
```

This example shows how to display all the MLS-hardware Layer 3-switching table IP entries:

```
Router#
show mls cef ip
Codes: decap - Decapsulation, + - Push Label
Index  Prefix              Adjacency
66     127.0.0.1/32         punt
67     10.1.1.100/32        punt
68     10.1.1.0/32          punt
```

```
69      10.1.1.255/32         punt
70      10.2.2.100/32         punt
71      10.2.2.0/32           punt
72      10.2.2.255/32         punt
73      10.2.2.5/32           Gi5/2,          0000.c005.0205
74      0.0.0.0/32            punt
75      10.255.255.255/32     punt
76      172.16.22.22/32       punt
77      172.20.0.0/32         punt
78      173.32.255.255/32     punt
79      172.16.1.153/32       Vl30,           0050.808b.8200
81      172.16.1.91/32        Vl30,           0004.4eef.8800
82      172.16.1.100/32       Vl30,           00d0.bb02.0400
83      172.17.223.3/32       Vl30,           00d0.061b.7000
84      172.22.5.3/32         Vl30,           00d0.061d.200a
85      172.16.1.101/32       Vl30,           0007.ecfc.e40a
86      172.20.100.1/32       Vl30,           0050.2a8d.700a
87      172.16.1.104/32       Vl30,           0050.0f2d.ac00
88      172.32.254.226/32     Vl30,           0050.2a8d.700a
89      10.2.2.7/32           Gi5/2,          0000.c005.0207
90      10.1.1.5/32           Gi5/1,          0000.0101.0105
3200    224.0.0.0/8           punt
3201    10.1.1.0/24           punt
3202    10.2.2.0/24           punt
134400 200.20.0.0/8           punt
134432 0.0.0.0/0              drop
524256 0.0.0.0/0              drop
Router#
```

The table below describes the fields shown in the examples.

Table 20: show mls cef ip Command Output Fields

Field	Description
Index	MLS-hardware Layer 3-switching table entry index; the maximum is 256,000 entries.
Prefix	Entry prefix address/mask.
Adjacency	Adjacency information.

This example shows how to display the detailed MLS-hardware Layer 3-switching table entries:

```
Router#
 show mls cef ip 127.0.0.1 detail
Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0,C0 - don't comp bit 0,V1 - Vlan 1,C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(194    ): E | 1 FFF  0 0 0 0   255.255.255.255
V(194    ): 8 | 1 0    0 0 0 0   127.0.0.1 (A:133120 ,P:1,D:0,m:0 ,B:0)
Router#
```

This example shows how to display all the prefixes that are configured for the statistic collection:

```
Router# show mls cef ip accounting per-prefix
     VRF              Prefix/Mask        Packets          Bytes
A - Active, I - Inactive
Router#
```

Related Commands

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

show mls cef ip multicast

To display the IP entries in the Multilayer Switching (MLS)-hardware Layer 3-switching table on the switch processor, use the **show mls cef ip multicast** command in user EXEC or privileged EXEC mode.

show mls cef ip multicast {**bidir**| **grp-only**| **source** *source-ip*} [**detail**| **group** *group-id*| **vlan** *rpf-vlanid*]

show mls cef ip multicast control [**detail**| **prefix** *prefix*| **vlan** *rpf-vlanid*]

show mls cef ip multicast group *group-id* [**detail**| **vlan** *rpf-vlanid*]

show mls cef ip multicast src-grp [**detail**| **group** *group-ip*| **source**| **vlan** *rpf-vlanid*]

show mls cef ip multicast subnet [**detail**| **prefix** *prefix*| **vlan** *rpf-vlanid*]

show mls cef ip multicast summary [*vpn-num*]

show mls cef ip multicast tcam [*prefix* **[mask]**] **[detail]** [**module** *num*] [**vrf** *src-ip* {*src-port*| *dst-ip*} [*dst-port*| **module** *num*]]

show mls cef ip multicast {**grp-mask**| **vlan** *rpf-vlanid*| **vpn** *vpn-id*} **[detail]**

Syntax Description

bidir	Displays bidirectional (Bidir) information.
grp-only	Displays hardware-entry information that is based on (*,G) shortcuts; see the "Usage Guidelines" section for additional information.
source *source-ip*	Displays hardware-entry information based on the specified source IP address.
detail	(Optional) Displays hardware-entry details.
group *group-id*	(Optional) Displays hardware-entry information that is based on the specified group IP address.
vlan *rpf-vlanid*	(Optional) Displays information for a specific Reverse Path Forwarding (RPF) VLAN ID; valid values are from 0 to 4095.
control	(Optional) Displays hardware-entry information that is based on (*,G/m) entries; see the "Usage Guidelines" section for additional information.
prefix *prefix*	(Optional) Displays hardware-entry information that is based on an IP subnet prefix.
src-grp	Displays hardware-entry information that is based on (S,G) shortcuts; see the "Usage Guidelines" section for additional information.

subnet	Displays hardware-entry information that is based on (S/m,*) shortcuts; see the "Usage Guidelines" section for additional information.
summary	Displays a summary of installed-hardware shortcuts.
tcam	Displays Cisco Express Forwarding table information in a compact format; see the "Usage Guidelines" section for additional information.
mask	(Optional) Displays hardware-entry information that is based on the specified subnet mask.
vrf *src-ip*	(Optional) Displays the numeric Virtual Private Network (VPN) routing and forwarding (VRF) ID for the specified source IP address.
src-port	(Optional) Layer 4 source port; valid values are from 0 to 65535.
dst-ip	(Optional) Destination IP address.
dst-port	(Optional) Layer 4 destination port; valid values are from 0 to 65535.
grp-mask	Displays hardware-entry information that is based on Bidir (*,G/m) shortcuts.
vpn *vpn-id*	Displays hardware-entry information that is based on the specified VPN ID; valid values are from 0 to 4095.

Command Modes

User EXEC (>) Privileged EXEC (#)

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 Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

For Cisco 7600 series routers that are configured with a Supervisor Engine 2, the only supported syntax for the **show mls cef ip multicast**command is **show mls cef ip** {**multicast tcam**[*prefix* [*mask*]} [**module** *num*]].

There are two Multicast Multilayer Switching (MMLS) modes, ingress and egress. The output displayed differs for each mode.

The hardware-entry types are as follows:

- {S/m,*}--Interface/mask (or subnet) entries that are used to catch a directly connected source.
- {*,G/m}--Groups that are served by the route processors as group/mask.
- {G,C}--G indicates a destination MAC address, which is derived from an IP-multicast address, and C indicates the ingress VLAN.
- {S,G,C}--S indicates the source IP address, G indicates the destination IP address, which is a multicast address, and C indicates the ingress VLAN, which is usually the RPF VLAN of the flow.
- {S,G}--Multicast-routing table entry that is maintained by the software or a multicast-forwarding table entry that is created in the Forwarding Information Base (FIB) table.
- {*,G}--Same as {S,G}, except that the source address is a wildcard.

The designated forwarder (DF) index field ranges from 1 to 4 and is an index into the acceptance (Protocol Independent Multicast [PIM] Route Processors (RPs) multiplied by the DF) table. The acceptance table is used with DF forwarding and is used to identify the set of DF interfaces for each of the four RPs in a VPN.

Examples

This example shows how to display ingress hardware-entry information that is based on Bidir (*,G/m) shortcuts:

```
Router# show mls cef ip multicast grp-mask
Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask     Destination/mask    RPF/DF  Flags #packets  #bytes   rwindex  Output
Vlans/Info
+---------------+-------------------+-------+-----+---------+--------+--------+-----------------+
*               226.2.2.0/24        Df0     BCp   0         0         -        Vl50 [1 oifs]
*               225.2.2.0/24        Df1     BCp   0         0         -        Vl51 [1 oifs]
*               227.2.2.0/24        Df1     BCp   0         0         -        Vl51 [1 oifs]
Found 3 entries. 3 are mfd entries
Router#
```

This example shows how to display detailed ingress hardware-entry information that is based on Bidir (*,G/m) shortcuts:

```
Router# show mls cef ip multicast grp-mask detail
(*, 226.2.2.0/24)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:0 AdjPtr:7,32775,65543,98311 FibRpfNf:0 FibRpfDf:0 FibAddr:0x100
        rwvlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x5
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x0005
          V E C:  50 I:0x00449
(*, 225.2.2.0/24)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:1 AdjPtr:8,32776,65544,98312 FibRpfNf:0 FibRpfDf:0 FibAddr:0x102
        rwvlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x6
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x0006
          V E C:  51 I:0x0044B
(*, 227.2.2.0/24)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:1 AdjPtr:19,32787,65555,98323 FibRpfNf:0 FibRpfDf:0 FibAddr:0x104
        rwvlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x7
        packets:0000000000000 bytes:000000000000000000
```

```
        Starting Offset: 0x0007
          V E C:  51 I:0x0044B
Found 3 entries. 3 are mfd entries
Router#
```

This example shows how to display ingress-Bidir information:

```
Router# show mls cef ip multicast bidir

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask         Destination/mask    RPF/DF  Flags #packets      #bytes
rwindex  Output Vlans/Info
+---------------+---------------+-----+----+---------+-------------+------+---------------------+
*                   225.2.2.2/32         Df1    BCp   0             0                    -
      Vl51,Vl30 [2 oifs]
*                   225.2.2.1/32         Df1    BCp   0             0                    -
      Vl51,Vl30 [2 oifs]
Found 2 entries. 2 are mfd entries
Router#
```

This example shows how to display detailed ingress-Bidir information:

```
Router# show mls cef ip multicast bidir detail

(*, 225.2.2.2)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:1 AdjPtr:10,32778,65546,98314 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE2
        rwvlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0xA
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x000A
          V  C:  51 I:0x004B5 P->19A0
        - V
          V E C:  30 I:0x0049B
(*, 225.2.2.1)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:1 AdjPtr:9,32777,65545,98313 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE0
        rwvlans:0 rwindex:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x8
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x0008
          V  C:  51 I:0x004B1 P->199C
        - V
          V E C:  30 I:0x00499
Found 2 entries. 2 are mfd entries
Router#
```

This example shows how to display egress hardware-entry information that is based on Bidir (*,G/m) shortcuts:

```
Router# show mls cef ip multicast grp-mask

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask         Destination/mask    RPF/DF  Flags #packets      #bytes
rwindex  Output Vlans/Info
+---------------+---------------+-----+----+---------+-------------+------+---------------------+
*                   225.2.2.0/24         Df0    BCp   0             0                    -

*                   225.2.2.0/24         -      Bpr   0             0                    0x4AE
    Vl51 [1 oifs]
*                   225.2.2.0/24         -      Br    0             0                    0x40E
    Vl51 [1 oifs]
*                   226.2.2.0/24         Df1    BCp   0             0                    -

*                   226.2.2.0/24         -      Bpr   0             0                    0x4AE
    Vl50 [1 oifs]
*                   226.2.2.0/24         -      Br    0             0                    0x40E
    Vl50 [1 oifs]
*                   227.2.2.0/24         Df0    BCp   0             0                    -
```

```
*                   227.2.2.0/24         -      Bpr   0             0                   0x4AE
    Vl51 [1 oifs]
*                   227.2.2.0/24         -      Br    0             0                   0x40E
    Vl51 [1 oifs]
Found 3 entries. 3 are mfd entries
Router#
```

This example shows how to display detailed egress hardware-entry information that is based on Bidir (*,G/m) shortcuts:

```
Router# show mls cef ip multicast grp-mask detail

(*, 225.2.2.0/24)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:0 AdjPtr:7,32775,65543,98311 FibRpfNf:0 FibRpfDf:0 FibAddr:0x120
        rwvlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
        fmt:recir l3rwvld:1 DM:0 mtu:1522 rwtype:RECIR
        packets:0000000000000 bytes:000000000000000000
        PI:1 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:8,32776,65544,98312 FibRpfNf:0 FibRpfDf:0 FibAddr:0x122
        rwvlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x5
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x0005
          V E C:  51 I:0x0044C
        PI:0 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:9,32777,65545,98313 FibRpfNf:0 FibRpfDf:0 FibAddr:0x124
        rwvlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x5
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x0005
          V E C:  51 I:0x0044C
(*, 226.2.2.0/24)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:1 AdjPtr:10,32778,65546,98314 FibRpfNf:0 FibRpfDf:0 FibAddr:0x126
        rwvlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
        fmt:recir l3rwvld:1 DM:0 mtu:1522 rwtype:RECIR
        packets:0000000000000 bytes:000000000000000000
        PI:1 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:11,32779,65547,98315 FibRpfNf:0 FibRpfDf:0 FibAddr:0x128
        rwvlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1C
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x001C
          V E C:  50 I:0x00447
        PI:0 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:12,32780,65548,98316 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12A
        rwvlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1C
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x001C
          V E C:  50 I:0x00447
(*, 227.2.2.0/24)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:0 AdjPtr:13,32781,65549,98317 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12C
        rwvlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
        fmt:recir l3rwvld:1 DM:0 mtu:1522 rwtype:RECIR
        packets:0000000000000 bytes:000000000000000000
        PI:1 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:14,32782,65550,98318 FibRpfNf:0 FibRpfDf:0 FibAddr:0x12E
        rwvlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1D
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x001D
          V E C:  51 I:0x0044C
        PI:0 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:15,32783,65551,98319 FibRpfNf:0 FibRpfDf:0 FibAddr:0x130
        rwvlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1D
        packets:0000000000000 bytes:000000000000000000
        Starting Offset: 0x001D
          V E C:  51 I:0x0044C
```

```
Found 3 entries. 3 are mfd entries
Router#
```

This example shows how to display egress-Bidir information:

```
Router# show mls cef ip multicast bidir

Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial,
       c - Central Rewrite, p - Primary Input, r - Recirculation
Source/mask         Destination/mask    RPF/DF  Flags #packets      #bytes
rwindex  Output Vlans/Info
+--------------+---------------+------+----+----------+-------------+------+-------------------+
*                  225.2.2.2/32         Df0    BCp   0             0                  -

*                 225.2.2.2/32         -      Bpr   0             0                  0x4AE
    Vl51,Vl30 [2 oifs]
*                 225.2.2.2/32         -      Br    0             0                  0x40E
    Vl51,Vl30 [2 oifs]
*                  225.2.2.1/32         Df0    BCp   0             0                  -

*                 225.2.2.1/32         -      Bpr   0             0                  0x4AE
    Vl51,Vl30 [2 oifs]
*                 225.2.2.1/32         -      Br    0             0                  0x40E
    Vl51,Vl30 [2 oifs]
Found 2 entries. 2 are mfd entries
Router#
```

This example shows how to display detailed egress-Bidir information:

```
Router# show mls cef ip multicast bidir detail

(*, 225.2.2.2)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:0 AdjPtr:19,32787,65555,98323 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE6
        rwvlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
        fmt:recir l3rwvld:1 DM:0 mtu:1522 rwtype:RECIR
        packets:000000000000 bytes:000000000000000000
        PI:1 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:20,32788,65556,98324 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE8
        rwvlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x22
        packets:000000000000 bytes:000000000000000000
        Starting Offset: 0x0022
          V  C:  51 I:0x004B3 P->24
          V E C:  30 I:0x004B6
        PI:0 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:21,32789,65557,98325 FibRpfNf:0 FibRpfDf:0 FibAddr:0xEA
        rwvlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x22
        packets:000000000000 bytes:000000000000000000
        Starting Offset: 0x0022
          V  C:  51 I:0x004B3 P->24
          V E C:  30 I:0x004B6
(*, 225.2.2.1)
        PI:1 (1) CR:0 (0) Recirc:0 (1)
        DFidx:0 AdjPtr:16,32784,65552,98320 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE0
        rwvlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
        fmt:recir l3rwvld:1 DM:0 mtu:1522 rwtype:RECIR
        packets:000000000000 bytes:000000000000000000
        PI:1 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:17,32785,65553,98321 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE2
        rwvlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1E
        packets:000000000000 bytes:000000000000000000
        Starting Offset: 0x001E
          V  C:  51 I:0x004AF P->20
          V E C:  30 I:0x004B2
        PI:0 (1) CR:0 (0) Recirc:1 (1)
        AdjPtr:18,32786,65554,98322 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE4
        rwvlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
        fmt:mcast l3rwvld:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1E
        packets:000000000000 bytes:000000000000000000
```

```
        Starting Offset: 0x001E
          V  C:  51 I:0x004AF P->20
          V E C:  30 I:0x004B2
Found 2 entries. 2 are mfd entries
Router#
```

This example shows how to display TCAM information:

```
Router# show mls cef ip multicast tcam

Index  Group              Source             RPF/DF Interface
64     224.0.1.39         0.0.0.0            NULL
66     224.0.1.40         0.0.0.0            NULL
96     224.0.0.0          0.0.0.0            NULL
Router#
```

show mls cef ipv6

To display the hardware IPv6-switching table entries, use the **show mls cef ipv6**command in privileged EXEC mode.

show mls cef ipv6 [**vrf** *vrf-name*] [*ip-address*/*mask*] [**accounting per-prefix**] [**module** *number*]

show mls cef ipv6 exact-route *src-addr* [*L4-src-port*] *dst-addr* [*L4-dst-port*]

show mls cef ipv6 multicast tcam [*v6mcast-address*] **[detail] [internal]**

Syntax Description

vrf	(Optional) IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name.
ip-address / *mask*	(Optional) Entry IPv6 address and prefix mask. Valid values for the *mask* argument are from 0 through 128.
accounting per-prefix	(Optional) Displays per-prefix accounting statistics.
module *number*	(Optional) Displays the entries for a specific module.
exact-route	Provides the exact route of IPv6-switching table entries.
src-addr	Source IP address.
L4-src-port	(Optional) Layer 4-source port number; valid values are from 0 to 65535.
dst-addr	Destination IP address.
L4-dst-port	(Optional) Layer 4-destination port number; valid values are from 0 to 65535.
multicast tcam	Displays IPv6-multicast entries.
v6mcast-address	(Optional) IPv6-multicast address.
detail	(Optional) Displays detailed hardware information.
internal	(Optional) *Displays internal hardware information.*

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	The output was changed to display multicast protocol information in the Forwarding Information Base (FIB) driver.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

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

You can enter this command on the supervisor engine and Multilayer Switching (MLS)-hardware Layer 3-switching module consoles only. Enter the **remote login** command to enter a session into the supervisor engine and distributed forwarding card (DFC)-equipped module to enter the commands.

When entering the *ip-address* / *mask* argument, use this format, X:X:X:X::X/*mask,*where valid values for *mask* are from 0 to 128.

Up to 64 IPv6 prefixes are supported.

You must enter the *L4-src-port* and *L4-dst-port* arguments when the load-sharing mode is set to full, for example, when Layer 4 ports are included in the load-sharing hashing algorithm.

Examples

This example shows how to display the hardware IPv6-switching table entries:

```
Router# show mls cef ipv6
Codes:M-MPLS encap, + - Push label
Index Prefix Adjacency
524384 BEEF:6::6/128 punt
524386 5200::6/128 punt
524388 2929::6/128 punt
524390 6363::30/128 Fa1/48 , 0000.0001.0002
524392 3FFE:1B00:1:1:0:5EFE:1B00:1/128 punt
524394 2002:2929:6:2::6/128 punt
524396 2002:2929:6:1::6/128 punt
524398 6363::6/128 punt
524416 BEEF:6::/64 drop
524418 5200::/64 punt
524420 2929::/64 punt
524422 2002:2929:6:2::/64 punt
524424 2002:2929:6:1::/64 punt
524426 6363::/64 punt
524428 3FFE:1B00:1:1::/64 Tu4 , V6 auto-tunnel
524448 FEE0::/11 punt
524480 FE80::/10 punt
524512 FF00::/8 punt
524544 ::/0 drop
```

This example shows how to display the IPv6 entries for a specific IPv6 address and mask:

```
Router# show mls cef ipv6 2001:4747::/64

Codes:R - Recirculation, I-IP encap
M-MPLS encap, + - Push label
```

```
Index Prefix Out i/f Out Label
160 2001:4747::/64 punt
```

This example shows how to display all the IPv6-FIB entries that have per-prefix statistics available:

```
Router#
show mls cef ipv6 accounting per-prefix
(I) BEEF:2::/64: 0 packets, 0 bytes
A - Active, I - Inactive
```

This example shows how to display detailed hardware information:

```
Router# show mls cef ipv6 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
D - FIB Don't short-cut, m - mod-num
Format: IPv6_DA - (C | xtag vpn uvo prefix)
M(128 ): F | 1 FF 1 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
V(128 ): C | 1 0 1 2001:4747::1253 (A:12 ,P:1,D:0,m:0 )
M(160 ): F | 1 FF 1 FFFF:FFFF:FFFF:FFFF::
V(160 ): C | 1 0 1 2001:4747:: (A:11 ,P:1,D:0,m:0 )
M(224 ): F | 1 FF 1 FFE0::
V(224 ): C | 1 0 1 FEE0:: (A:11 ,P:1,D:0,m:0 )
M(256 ): F | 1 FF 1 FFC0::
V(256 ): C | 1 0 1 FE80:: (A:12 ,P:1,D:0,m:0 )
M(352 ): F | 1 FF 1 FF00::
V(352 ): C | 1 0 1 FF00:: (A:12 ,P:1,D:0,m:0 )
M(480 ): F | 1 FF 1 ::
V(480 ): C | 1 0 1 :: (A:14 ,P:1,D:0,m:0
```

Related Commands

Command	Description
mls ipv6 acl compress address unicast	Turns on the compression of IPv6 addresses.
remote login	Accesses the Cisco 7600 series router console or a specific module.

show mls cef ipx

To display Internetwork Packet Exchange (IPX) entries in the Multilayer Switching (MLS)-hardware Layer 3 switching table, use the **show mls cef ipx** command in user EXEC or privileged EXEC mode.

show mls cef ipx [*prefix* [*mask*| **module** *number*]| **module** *number*]

Syntax Description

prefix	(Optional) Entry prefix in the format A.B.C.D.
mask	(Optional) Entry prefix mask in the format A.B.C.D.
module *number*	(Optional) Displays the entries for a specific module.

Command Modes

User EXEC(>) Privileged EXEC (#)

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

Information in the output of the **show mls cef ipx** command is also displayed in the **show mls ipx** command.

Examples

This example shows how to display the IPX entries in the MLS-hardware Layer 3-switching table. The fields shown in the display are self-explanatory.

```
Router# show mls cef ipx
Router#
Index      Prefix           Mask               Adjacency
.
```

Related Commands

Command	Description
show mls ipx	Displays IPX-related MLS-hardware Layer 3 switching table entries.

show mls cef logging

To display the contents of the ternary content addressable memory (TCAM)-inconsistency buffer, use the **show mls cef logging** command in user EXEC or privileged EXEC mode.

show mls cef logging [**module** *number*]

Syntax Description

module *number*	(Optional) Displays the entries for a specific module.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
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.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

In Cisco 7600 series routers that are configured with a Supervisor Engine 2 with a Policy Feature Card (PFC) and a Multilayer Switch Feature Card 2 (MSFC2), multilayer switching (MLS)-hardware Layer 3 switching provides IP unicast and IP multicast Layer 3 switching for a Supervisor Engine 2, a Policy Feature Card 2 (PFC2), an MSFC2, and fabric-enabled switching modules that have a Distributed Forwarding Card (DFC).

The TCAM-inconsistency buffer records any inconsistency that is found in the TCAM.

MLS-hardware Layer 3 switching applies to IP traffic only.

Examples

This example shows how to display the contents of the TCAM inconsistency buffer. The significant fields shown in the display are self-explanatory.

```
Router# show mls cef logging

PFIB_ERR:TCAM_SHADOW_CONSISTENCY_ERR:value : Index: 100
Expected: 0 -0 -0
Hardware: 5 -1020304 -0
PFIB_ERR:TCAM_SHADOW_CONSISTENCY_ERR:Mask : Index: 3
Expected: 4 -0 -0
Hardware: 6 -FFF00000-0
```

show mls cef lookup

To display the IP entries in the multilayer switching (MLS)-hardware Layer 3 switching table for the specified destination IP address, use the **show mls cef lookup** command in user EXEC or privileged EXEC mode.

show mls cef [ip] lookup *address* **[detail]** [**module** *number*]

Syntax Description

ip	(Optional) Displays IP entries in the MLS-hardware Layer 3-switching table; see the "Usage Guidelines" section for additional information.
address	IP address in the format A.B.C.D.
detail	(Optional) Displays hardware-entry details.
module *number*	(Optional) Displays the entries for a specific module.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

The lookup is performed as a "longest-prefix match" and displays the ternary content addressable memory (TCAM)-entry index that applies to the specified destination IP address.

The information output is in this format: Index, Prefix, Mask, and Adjacency.

The output of the **show mls cef lookup ip** and the **show mls cef lookup** commands is identical.

Examples

This example shows how to display the longest prefix match that applies to a specific IPv4-unicast address. The fields shown in the display are self-explanatory.

```
Router# show mls cef lookup 224.0.0.0
Codes: decap - Decapsulation, + - Push Label
Index  Prefix              Adjacency
3200   224.0.0.0/24        punt
```

show mls cef mac

To display the multilayer switching (MLS)-hardware Layer 3-switching MAC-address information for the MSFC, use the **show mls cef mac** command in user EXEC or privileged EXEC mode.

show mls cef mac [**module** *num*]

Syntax Description

module *num*	(Optional) Displays the entries for a specific module.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
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.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

In Cisco 7600 series routers that are configured with a Supervisor Engine 2 with a Policy Feature Card (PFC) and a Multilayer Switch Feature Card 2 (MSFC2), multilayer switching (MLS)-hardware Layer 3 switching provides IP unicast and IP multicast Layer 3 switching for a Supervisor Engine 2, a Policy Feature Card 2 (PFC2), an MSFC2, and fabric-enabled switching modules that have a Distributed Forwarding Card (DFC).

Examples

This example shows how to display the MLS-hardware Layer 3-switching MAC-address information for the MSFC. The fields shown in the display are self-explanatory.

```
Router#
show mls cef mac
Router MAC address:00d0.061d.200a
```

Related Commands

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

Command	Description
show mls cef summary	Displays the number of routes in the MLS-hardware Layer 3-switching table for all the protocols.

show mls cef maximum-routes

To display the current maximum-route system configuration, use the **show mls cef maximum-routes** command in user EXEC or privileged EXEC mode.

show mls cef maximum-routes

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

When you enter the **mls cef maximum-routes** command to change the configuration, the following additional fields appear in the output of the **show mls cef maximum-routes** command:

- User configured--Shows configuration changes that you have made.
- Upon reboot--Shows the configuration after a system reboot.

These fields appear if you have not saved the change (using the **copy system:running-config nvram: startup-config** command) after entering the **mls cef maximum-routes** command. See the "Examples" section for additional information.

Examples

This section contains examplse of the **msl cef maximum-routes** command. The fields shown in the display are self-explanatory.

This example shows the display after you have entered the **mls cef maximum-routes**command, saved the change (**copy system:running-config nvram: startup-config** command), and rebooted the system:

```
Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=========================
Current :-
-------
IPv4 - 1k (default)
```

```
MPLS - 239k
IPv6 + IP Multicast - 8k (default)
```

This example shows the display if you entered the **mls cef maximum-routes** command and did not save the change:

```
Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=========================
Current :-
-------
IPv4 - 1k (default)
MPLS - 239k
IPv6 + IP Multicast - 8k (default)
User configured :-
---------------
IPv4 + MPLS - 192k (default)
IPv6 + IP multicast - 32k (default)
Upon reboot :-
-----------
IPv4 - 1k (default)
MPLS - 239k
IPv6 + IP multicast - 8k (default)
```

This example shows the output if you have made a configuration change and saved the change (**copy system:running-config nvram: startup-config** command):

```
Router# show mls cef maximum-routes
FIB TCAM maximum routes :
=========================
Current :-
-------
IPv4 - 1k (default)
MPLS - 239k
IPv6 + IP Multicast - 8k (default)
User configured :-
---------------
IPv4 + MPLS - 192k (default)
IPv6 + IP multicast - 32k (default)
```

Related Commands

Command	Description
copy system:running-config nvram: startup-config	Saves the configuration to NVRAM.
mls cef maximum-routes	Limits the maximum number of the routes that can be programmed in the hardware allowed per protocol.

show mls cef mpls

To display the Multiprotocol Label Switching (MPLS) entries in the Multilayer Switching (MLS)-hardware Layer 3 switching table, use the **show mls cef mpls** command in user EXEC or privileged EXEC mode.

show mls cef mpls [detail] [internal] [**labels** *value*] [**module** *number*] [**vpn** *instance*] [**vrf** *instance*]

Syntax Description

detail	(Optional) Displays hardware-entry details.
internal	(Optional) Displays internal Cisco Express Forwarding entries.
labels *value*	(Optional) Displays the entries for a specific label; valid values are from 0 to 1048575.
module *number*	(Optional) Displays the entries for a specific module.
vpn *instance*	(Optional) Displays the Virtual Private Network (VPN) ID MPLS table entries for a specific VPN instance; valid values are from 0 to 4095.
vrf *instance*	(Optional) Displays the MPLS Cisco Express Forwarding table entries for a specific VPN routing and forwarding (VRF) instance.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This examples shows how to display MPLS entries. The fields shown in the display are self-explanatory.

```
Router# show mls cef mpls

Codes: + - Push label, - - Pop Label          * - Swap Label
Index  Local     Label                 Out i/f
       Label      Op
```

show mls cef rpf

To display the information about the Reverse Path Forwarding (RPF) hardware in the Multilayer Switching (MLS)-hardware Layer 3-switching table, use the **show mls cef rpf** command in user EXEC or privileged EXEC mode.

show mls cef [ip] rpf [*ip-address*] [**module** *num*]

Syntax Description

ip	(Optional) Displays IP entries in the MLS-hardware Layer 3-switching table; see the "Usage Guidelines" section for additional information.
ip-address	(Optional) IP address.
module *num*	(Optional) Displays the entries for a specific module.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

If you enter the **show mls cef ip rpf** command without arguments, the RPF global mode status is displayed.

The output of the **show mls cef ip rpf** and the **show mls cef rpf** commands is identical.

Examples

This example shows how to display the status of the RPF global mode. The fields shown in the display are self-explanatory.

```
Router# show mls cef rpf
RPF global mode:        not enabled
Router#
```

This example shows how to display the RPF information for a specific IP address. The fields shown in the display are self-explanatory.

```
Router# show mls cef rpf 10.100.0.0
RPF information for prefix 10.100.0.0/24
uRPF check performed in the hardware for interfaces :
GigabitEthernet1/1
Router#
```

Related Commands

Command	Description
mls ip cef rpf multipath	Configures the RPF modes.

show mls cef statistics

To display the number of switched packets and bytes, use the **show mls cef statistics** command in user EXEC or privileged EXEC mode.

show mls cef statistics [**module** *number*]

Syntax Description

module *number*	(Optional) Displays the information for a specific module.

Command Modes

User EXEC (>) Privileged EXEC (#)

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.

Usage Guidelines

In Cisco 7600 series routers that are configured with a Supervisor Engine 2 with a Policy Feature Card (PFC) and a Multilayer Switching Feature Card 2 (MSFC2), Multilayer Switching (MLS)-hardware Layer 3 switching provides IP unicast and IP multicast Layer 3 switching for a Supervisor Engine 2, a PFC2, an MSFC2, and fabric-enabled switching modules that have a Distributed Forwarding Card (DFC).

Examples

This example shows how to display the MLS-hardware Layer 3-switching statistics. The fields shown in the display are self-explanatory.

```
Router# show mls cef statistics
Total CEF switched packets:  0000000000000000
Total CEF switched bytes:    0000000000000000
Router#
```

show mls cef summary

To display the number of routes in the Multilayer Switching (MLS)-hardware Layer 3-switching table for all the protocols, use the **show mls cef summary** command in user EXEC or privileged EXEC mode.

show mls cef summary [**module** *number*]

Syntax Description

module *number*	(Optional) Displays the information for a specific module.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The output was changed and no longer displays the Cisco Express Forwarding switched packets and bytes total.
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(33)SXI	The output was changed for display of VRF and non-VRF routes for both IPv4 and IPv6 routes.

Usage Guidelines

The number of prefixes in the MLS-hardware Layer 3-switching table indicates the individual numbers for IPv4 and IPv6 unicast, IPv4 multicast, Multiprotocol Label Switching (MPLS), and EoM routes.

For Cisco 7600 series routers that are configured with a Supervisor Engine 2, the output displays the CEF-switched packets and total bytes.

When IPv6 is not configured, the command output from a Cisco Catalyst 6500 series switch running Cisco IOS Release 12.2(33)SXI or a later release will show 255 IPv6 VRF routes.

Examples

Examples

This example shows the output from Cisco 7600 series routers that are configured with a Supervisor Engine 720.

This example shows how to display a summary of MLS-hardware Layer 3-switching information:

```
Router#
show mls cef summary
Total routes:               80385
    IPv4 unicast routes:          42
    IPv4 Multicast routes:        5
    MPLS routes:                  0
    IPv6 unicast routes:          2
    EoM routes:                   0
Router#
```

Examples

This example shows the output from Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This example shows how to display a summary of MLS-hardware Layer 3-switching information:

```
Router#
show mls cef summary
Total CEF switched packets: 0000000000098681
Total CEF switched bytes:   0000000004539326
Total routes:               80385
    IP unicast routes:      80383
    IPX routes:             0
    IP multicast routes:    2
Router#
```

Examples

This example shows the output from a Cisco Catalyst 6500 series switch running Cisco IOS Release 12.2(33)SXI or a later release:

```
Router# show mls cef summary
Total routes:                   280
    IPv4 unicast routes:        20
        IPv4 non-vrf routes :   9
        IPv4 vrf routes :       11
    IPv4 Multicast routes:      3
    MPLS routes:                0
    IPv6 unicast routes:        257
        IPv6 non-vrf routes:    2
        IPv6 vrf routes:        255
    IPv6 multicast routes:      3
    EoM routes:                 0
```

The table below describes the fields in the **show mls cef summary**command output.

Table 21: show mls cef summary Command Output Fields

Field	Description
Total MLS-hardware Layer 3-switching switched packets	Number of MLS-hardware Layer 3-switching packets forwarded by the MLS-hardware Layer 3-switching engine.
Total MLS-hardware Layer 3-switching switched bytes	Number of bytes forwarded by the MLS-hardware Layer 3-switching engine.
Total routes	Number of route entries.
IP unicast routes	Number of IP-unicast route entries.

Field	Description
IP VRF routes	Number of virtual routing and forwarding (VRF) route entries.
IPX routes	Number of Internetwork Packet Exchange (IPX) route entries.
IP multicast routes	Number of IP-multicast route entries.

Related Commands

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

show mls cef vrf

To display information about the Virtual Private Network (VPN) routing and forwarding instance (VRF) Cisco Express Forwarding table for a specific VRF name, use the **show mls cef vrf** command in user EXEC or privileged EXEC mode.

show mls cef vrf *instance-name* [*prefix*] **[detail]** [**lookup** *ip-address*] [**module** *num*] [**rpf** [*ip-address*]]

Syntax Description

instance-name	VPN routing/forwarding instance name; valid values are from 0 to 4095.
prefix	(Optional) Prefix of the entry to display.
detail	(Optional) Displays the hardware-entry details.
lookup *ip-address*	(Optional) Displays the longest prefix-match lookup entry for the specified address.
module *num*	(Optional) Displays the entries for a specific module.
rpf *ip-address*	(Optional) Displays the unicast Reverse Path Forwarding (uRPF) check information for the (optional) specified IP address.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

The **show mls cef ip** command displays the Cisco Express Forwarding entries in the default VRF. To display specific (non-default) VRF entries, use the **show mls cef** [**ip**] **vrf** *vrf-name* command.

Examples

This example shows how to display information about the VPN routing and forwarding instance Cisco Express Forwarding table for a specific VRF name. The fields shown in the display are self-explanatory.

```
Router#
 show mls cef vrf vpn-1
```

```
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 0.0.0.0/32 receive
65 255.255.255.255/32 receive
280 10.50.27.1/32 receive
281 10.50.27.0/32 receive
282 10.50.27.255/32 receive
298 10.1.1.1/32 receive
299 10.1.1.0/32 receive
300 10.1.1.255/32 receive
656 10.1.99.1/32 receive
Router#
```

Related Commands

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

show mls ip cef rpf-table

To display the configuration of the Reverse Path Forwarding (RPF) Cisco Express Forwarding table, use the **show mls ip cef rpf-table**command in privileged EXEC mode.

show mls ip cef rpf-table

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

Examples

This example shows how to display the RPF Cisco Express Forwarding table entries. The fields shown in the display are self-explanatory.

```
Router#
show mls ip cef rpf-table
------------------------------------------------------------------------------
172.16.10.0/24       [0] Fa2/1, Fa2/2, Fa2/3, Fa2/4
172.16.20.0/24
172.16.30.0/24
10.10.0.0/16         [1] Gi1/1, Gi1/2
10.20.0.0/16
```

Related Commands

Command	Description
mls ip cef rpf interface-group	Defines an interface group in the RPF-VLAN table.

show mls ip non-static

To display information for the software-installed nonstatic entries, use the **show mls ip non-static** command in user EXEC or privileged in the EXEC mode.

show mls ip non-static [**count** [**module** *number*]| **detail** [**module** *number*]| **module** *number*]

Syntax Description

count	(Optional) Displays the total number of nonstatic entries.
module *number*	(Optional) Designates the module number.
detail	(Optional) Specifies a detailed per-flow output.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	This command is replaced by the **show mls netflow ip** command.

Usage Guidelines

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

Examples

This sections contains examples from the **show mls ip non-static** command. The fields shown in the display are self-explanatory.

This example shows how to display the software-installed nonstatic entries:

```
Router> show mls ip non-static
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed information for the software-installed nonstatic entries:

```
Router> show mls ip non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
```

```
Pkts          Bytes       Age   LastSeen  Attributes
-------------------------------------------------
QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+-----------+
Router>
```

This example shows how to display the total number of software-installed nonstatic entries:

```
Router> show mls ip non-static count
Displaying Netflow entries in Supervisor Earl
 Number of shortcuts = 0
Router>
```

show mls ip routes

To display the NetFlow routing entries, use the **show mls ip routes**command in user EXEC or privileged EXEC mode.

show mls ip routes [**non-static**| **static**] [**count** [**module** *number*]| **detail** [**module** *number*]| **module** *number*]

Syntax Description

non-static	(Optional) Displays the software-installed nonstatic entries.
static	(Optional) Displays the software-installed static entries.
count	(Optional) Displays the total number of NetFlow routing entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
detail	(Optional) Specifies a detailed per-flow output.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	This command is replaced by the **show mls netflow ip sw-installed** command

Usage Guidelines

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

Examples

This section contains examples of the **show mls ip routes non-static** command. The fields shown in the display are self-explanatory.

This example shows how to display the software-installed nonstatic routing entries:

```
Router> show mls ip routes non-static
```

```
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed information for the software-installed nonstatic routing entries:

```
Router> show mls ip routes non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+-----------+
Router>
```

This example shows how to display the total number of software-installed routing entries:

```
Router> show mls ip routes count
Displaying Netflow entries in Supervisor Earl
 Number of shortcuts = 0
Router>
```

Related Commands

Command	Description
show mls netflow ip sw-installed	Displays information for the software-installed IP entries.

show mls ip static

To display the information for the software-installed static IP entries, use the **show mls ip static** command in user EXEC or privileged EXEC mode.

show mls ip static [**count** [**module** *number*]| **detail** [**module** *number*]| **module** *number*]

Syntax Description

count	(Optional) Displays the total number of static entries.
module *number*	(Optional) Designates the module number.
detail	(Optional) Specifies a detailed per-flow output.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	This command is replaced by the **show mls netflow ip sw-installed** command.

Usage Guidelines

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

Examples

This section contains examples from the **show mls ip static**command. The fields shown in the display are self-explanatory.

This example shows how to display the software-installed static entries:

```
Router> show mls ip static
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed information for the software-installed static entries:

```
Router> show mls ip static detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
```

```
Pkts          Bytes       Age   LastSeen  Attributes
-------------------------------------------------
    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+-----------+
Router>
```

This example shows how to display the total number of software-installed static entries:

```
Router> show mls ip static count
Displaying Netflow entries in Supervisor Earl
 Number of shortcuts = 0
Router>
```

show mls ip statistics

To display the statistical information for the NetFlow IP entries, use the **show mls ip statistics** command in the user EXEC or privileged EXEC mode.

show mls ip statistics [**count** [**module** *number*]| **detail** [**module** *number*]| **module** *number*]

Syntax Description

count	(Optional) Displays the total number of NetFlow entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module.
detail	(Optional) Specifies a detailed per-flow output.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	On Cisco 7600 series routers that are configured with a Supervisor Engine 720, this command is replaced by the **show mls netflow ip** command.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

Examples

This section contains examples from the **show mls ip statistics** command. The fields shown in the display are self-explanatory.

This example shows how to display statistical information for the NetFlow IP entries:

```
Router> show mls ip statistics
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed statistical information for the NetFlow IP entries:

```
Router> show mls ip statistics detail
Displaying Netflow entries in Supervisor Earl
```

```
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
----------+------------+---------+-----------+----+-------+-------+----------+
Router>
```

show mls table-contention

To display table contention level (TCL) information, use the **show mls table-contention** command in the user EXEC or privileged EXEC mode.

show mls table-contention {**detailed**| **summary**| **aggregate**}

Syntax Description

detailed	Displays the detailed TCL information.
summary	Displays the TCL level.
aggregate	Displays the aggregate count of all missed flows in the Supervisor Engine 720 and page hits or misses in Supervisor Engine 2.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to include the following: • The **aggregate** keyword • The last reading of the corresponding registers in the **summary** and **detailed** keywords
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

Usage Guidelines

You can enter the **aggregate** keyword to display the statistics for the NetFlow-creation failures and NetFlow-hash aliases in the Supervisor Engine 720.

You can enter the **aggregate** keyword to display the page hits and misses in the Supervisor Engine 2.

The last reading of the corresponding registers are displayed in the **summary** and **detailed** keywords for the Supervisor Engine 720.

Examples

This section contains examples from the **show mls table-contention** command. The fields shown in the display are self-explanatory.

This example shows how to display a detailed list of TCL information:

```
Router#
show mls table-contention detailed
Detailed Table Contention Level Information
==========================================
Layer 3
-------
L3 Contention Level:     0
Page Hits Requiring 1 Lookup    =        31
Page Hits Requiring 2 Lookups   =        0
Page Hits Requiring 3 Lookups   =        0
Page Hits Requiring 4 Lookups   =        0
Page Hits Requiring 5 Lookups   =        0
Page Hits Requiring 6 Lookups   =        0
Page Hits Requiring 7 Lookups   =        0
Page Hits Requiring 8 Lookups   =        0
Page Misses                     =        0
Router#
```

This example shows how to display a summary of TCL information:

```
Router# show mls table-contention summary
Summary of Table Contention Levels (on a scale of 0 (lowest) to 3 (highest))
================================================================================
L3 Contention Level: 0
```

This example shows how to display an aggregate count of all missed flows in the Supervisor Engine 720 and page hits/misses in Supervisor Engine 2:

```
Router# show mls table-contention aggregate
Earl in Module 1
Detailed Table Contention Level Information
==========================================
Layer 3
-------
L3 Contention Level:     0
Page Hits Requiring 1 Lookup    =        24000
Page Hits Requiring 2 Lookups   =        480
Page Hits Requiring 3 Lookups   =        0
Page Hits Requiring 4 Lookups   =        0
Page Hits Requiring 5 Lookups   =        0
Page Hits Requiring 6 Lookups   =        0
Page Hits Requiring 7 Lookups   =        0
Page Hits Requiring 8 Lookups   =        0
Page Misses                     =        0
```

show monitor event-trace

To display event trace messages for Cisco IOS software subsystem components, use the **show monitor event-trace** command in privileged EXEC mode.

show monitor event-trace {**all-traces [merged]** {**all**| **back** {*mmm* | *hhh*:*mm*}| **clock** *hh*:*mm* [*date month*| *month date*]| **from-boot** *seconds*| **latest**}| *component* {**all**| **back** {*mmm* | *hh*:*mm*| [*date month*| *month date*]}| **clock** *hh*:*mm* [*date month*| *month date*]| **from-boot** *seconds*| **latest**| **parameters**}} **[detail]**

Syntax Description

all-traces	(Optional) Displays all event trace messages in memory to the console.
merged	(Optional) Displays all event traces entries sorted by time.
all	Displays all event trace messages currently in memory.
back {*mmm* | *hhh:mm*}	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes. The time argument is specified either in minutes or in hours and minutes format (mmm or hh:mm).
clock *hh:mm*	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
date	(Optional) Day of the month.
month	(Optional) Displays the month of the year.
from-boot *seconds*	Displays event trace messages starting from a specified number of seconds after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace** *component* **from-boot ?** command.
latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
component	(Optional) Name of the Cisco IOS software subsystem component that is the object of the event trace. To get a list of components that support event tracing in this release, use the **monitor event-trace ?** command.
parameters	Displays the trace parameters. The only parameter displayed is the size (number of trace messages) of the trace file.

detail	(Optional) Displays detailed trace information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The **show monitor event-trace cef** comand replaced the **show cef events**and **show ip cef events** commands.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. The **spa** component keyword was added to support online insertion and removal (OIR) event messages for shared port adapters (SPAs). The **bfd** keyword was added for the *component* argument to display trace messages relating to the Bidirectional Forwarding Detection (BFD) feature.
12.4(4)T	Support for the **bfd** keyword was added for Cisco IOS Release 12.4(4)T.
12.0(31)S	Support for the **bfd** keyword was added for Cisco IOS Release 12.0(31)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.4(9)T	The **cfd** keyword was added as an entry for the *component* argument to display trace messages relating to crypto fault detection.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information.

The trace function is not locked while information is being displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace** command will generate a message

indicating that some messages might be lost; however, messages will continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace**command will stop displaying messages.

Use the **bfd** keyword for the *component* argument to display trace messages relating to the BFD feature.

Use the **cfd** keyword for the *component* argument to display trace messages relating to the crypto fault detection feature. This keyword displays the contents of the error trace buffers in an encryption data path.

Examples

Examples

The following is sample output from the **show monitor event-trace** *component* command for the interprocess communication (IPC) component. Notice that each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace ipc

3667:  6840.016:Message type:3 Data=0123456789
3668:  6840.016:Message type:4 Data=0123456789
3669:  6841.016:Message type:5 Data=0123456789
3670:  6841.016:Message type:6 Data=0123456
```

Examples

Use the **show monitor event-trace bfd all**command to display logged messages for important BFD events in the recent past. The following trace messages show BFD session state changes:

```
 Router# show monitor event-trace bfd all
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], event Session
            create, state Unknown -> Fail
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Fail -> Down
             (from LC)
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Down -> Init
             (from LC)
     3d03h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,1], state Init -> Up
            (from LC)
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], event Session
            create, state Unknown -> Fail
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Fail -> Down
             (from LC)
     3d07h: EVENT: Session [172.16.10.2,172.16.10.1,Fa6/0,2], state Down -> Up
            (from LC)
```

To display trace information for all components configured for event tracing on the networking device, enter the **show monitor event-trace all-traces** command. In this example, separate output is provided for each event, and message numbers are interleaved between the events.

```
Router# show monitor event-trace all-traces

Test1 event trace:
3667: 6840.016:Message type:3 Data=0123456789
3669: 6841.016:Message type:4 Data=0123456789
3671: 6842.016:Message type:5 Data=0123456789
3673: 6843.016:Message type:6 Data=0123456789
Test2 event trace:
3668: 6840.016:Message type:3 Data=0123456789
3670: 6841.016:Message type:4 Data=0123456789
3672: 6842.016:Message type:5 Data=0123456789
3674: 6843.016:Message type:6 Data=0123456789
```

Examples

The following is sample output from the **show monitor event-trace** *component* **latest** command for the **spa** component:

```
Router# show monitor event-trace spa latest
00:01:15.364: subslot 2/3: 4xOC3 POS SPA, TSM Event:inserted  New state:wait_psm
_ready
     spa type 0x440
00:02:02.308: subslot 2/0: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/0: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/1: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/1: not present, TSM Event:remove_complete  New state:idle
00:02:02.308: subslot 2/2: not present, TSM Event:empty  New state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.308: subslot 2/2: not present, TSM Event:remove_complete  New state:idle
00:02:02.312: subslot 2/3: not present(plugin 4xOC3 POS SPA), TSM Event:empty  New
state:remove
     spa type 0x0, fail code 0x0(none)
00:02:02.312: subslot 2/3: not present, TSM Event:remove_complete  New state:idle
```

Examples

If you select Cisco Express Forwarding as the component for which to display event messages, you can use the following additional arguments and keywords: **show monitor event-trace cef** [**events** | **interface** | **ipv6** | **ipv4**][**all**].

The following example shows the IPv6 or IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv6 all
00:00:24.612:  [Default] *::*/*'00             New FIB table          [OK]
Router# show monitor event-trace cef ipv4 all
00:00:24.244:  [Default] 127.0.0.81/32'01       FIB insert             [OK]
```

In the following example, all event trace messages for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all
00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.612: SubSys  ipv6fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following example shows Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all
00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
```

```
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet0/1(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

Examples

The following example shows the IPv4 events related to the Cisco Express Forwarding component. Each trace message is numbered and is followed by a time stamp (derived from the device uptime). Following the time stamp is the component-specific message data.

```
Router# show monitor event-trace cef ipv4 all
00:00:48.244:  [Default] 127.0.0.81/32'01      FIB insert                [OK]
```

In the following example, all event trace message for the Cisco Express Forwarding component are displayed:

```
Router# show monitor event-trace cef events all
00:00:18.884: SubSys  fib_ios_chain init
00:00:18.884: Inst    unknown -> RP
00:00:24.584: SubSys  fib init
00:00:24.592: SubSys  fib_ios init
00:00:24.592: SubSys  fib_ios_if init
00:00:24.596: SubSys  ipv4fib init
00:00:24.608: SubSys  ipv4fib_ios init
00:00:24.620: Flag    IPv4 CEF enabled set to yes
00:00:24.620: Flag    0x7BF6B62C set to yes
00:00:24.620: Flag    IPv4 CEF switching enabled set to yes
00:00:24.624: GState  CEF enabled
00:00:24.628: SubSys  ipv4fib_les init
00:00:24.628: SubSys  ipv4fib_pas init
00:00:24.632: SubSys  ipv4fib_util init
00:00:25.304: Process Background created
00:00:25.304: Flag    IPv4 CEF running set to yes
00:00:25.304: Process Background event loop enter
00:00:25.308: Flag    IPv4 CEF switching running set to yes
```

The following examples show Cisco Express Forwarding interface events:

```
Router# show monitor event-trace cef interface all

00:00:24.624: <empty>      (sw  4) Create   new
00:00:24.624: <empty>      (sw  4) SWIDBLnk FastEthernet1/0/0(4)
00:00:24.624: Fa0/0        (sw  4) NameSet
00:00:24.624: <empty>      (hw  1) Create   new
00:00:24.624: <empty>      (hw  1) HWIDBLnk FastEthernet1/0/0(1)
00:00:24.624: Fa0/0        (hw  1) NameSet
00:00:24.624: <empty>      (sw  3) Create   new
00:00:24.624: <empty>      (sw  3) SWIDBLnk FastEthernet1/1/0(3)
00:00:24.624: Fa0/1        (sw  3) NameSet
00:00:24.624: <empty>      (hw  2) Create   new
```

Examples

To troubleshoot errors in an encryption datapath, enter the **show monitor event-trace cfd all**command. In this example, events are shown separately, each beginning with a time stamp, followed by data from the error trace buffer. Cisco Technical Assistence Center (TAC) engineers can use this information to diagnose the cause of the errors.

Note If no packets have been dropped, this command does not display any output.

```
Router# show monitor event-trace cfd all
00:00:42.452: 450000B4 00060000 FF33B306 02020203 02020204 32040000 F672999C
        00000001 7A7690C2 A0A4F8BC E732985C D6FFDCC8 00000001 C0902BD0
        A99127AE 8EAA22D4
```

```
00:00:44.452: 450000B4 00070000 FF33B305 02020203 02020204 32040000 F672999C
        00000002 93C01218 2325B697 3C384CF1 D6FFDCC8 00000002 BFA13E8A
        D21053ED 0F62AB0E
00:00:46.452: 450000B4 00080000 FF33B304 02020203 02020204 32040000 F672999C
        00000003 7D2E11B7 A0BA4110 CC62F91E D6FFDCC8 00000003 7236B930
        3240CA8C 9EBB44FF
00:00:48.452: 450000B4 00090000 FF33B303 02020203 02020204 32040000 F672999C
        00000004 FB6C80D9 1AADF938 CDE57ABA D6FFDCC8 00000004 E10D8028
        6BBD748F 87F5E253
00:00:50.452: 450000B4 000A0000 FF33B302 02020203 02020204 32040000 F672999C
        00000005 697C8D9D 35A8799A 2A67E97B D6FFDCC8 00000005 BC21669D
        98B29FFF F32670F6
00:00:52.452: 450000B4 000B0000 FF33B301 02020203 02020204 32040000 F672999C
        00000006 CA18CBC4 0F387FE0 9095C27C D6FFDCC8 00000006 87A54811
        AE3A0517 F8AC4E64
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show monitor event-trace adjacency

To display adjacency trace events, use the **show monitor event-trace adjacency** command in privileged EXEC mode.

show monitor event-trace adjacency {{**all**| **back** *trace-duration*| **clock** *hh* **:** *mm* [*date*] [*month*]| **from-boot** [*seconds*]| **latest**} **[detail]| parameters**}

Syntax Description

all	Displays all event trace messages in the current buffer.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
trace-duration	The time duration in hours and minutes format (mmm or hhh:mm).
clock *hh* **:** *mm*	Displays event trace messages starting from a specified time in hours and minutes format (hh:mm).
date	(Optional) Day of the month from 1 to 31.
month	(Optional) Month of the year.
from-boot	Displays event trace messages starting after booting up (uptime).
seconds	(Optional) The specified number of seconds following bootup (uptime) after which event trace messages should start being displayed. The range is from 0 to 785.
latest	Displays the latest trace events since last display.
detail	(Optional) Displays detailed trace information.
parameters	Displays the parameters configured for the trace.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(18)T	This command was integrated into Cisco IOS Release 12.4(18)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show monitor event-trace adjacency all** command. The fields are self-explanatory.

```
Router# show monitor event-trace adjacency all

*Aug  7 05:13:56.408: GLOBAL: adj system chunk pool created (element size 276) [OK]
*Aug  7 05:13:56.408: GLOBAL: adj system state change to adjacency system up [OK]
*Aug  7 05:13:56.408: GLOBAL: adj manager background process started [OK]
*Aug  7 05:13:56.408: GLOBAL: adj ios manager up [OK]
*Aug  7 05:13:56.408: GLOBAL: adj ios manager add enable [OK]
*Aug  7 05:13:56.924: GLOBAL: adj ipv4 bundle changed to IPv4 no fixup, no
                      redirect adj oce [OK]
*Aug  7 05:14:07.928: GLOBAL: adj mgr notified of fibidb state change int
                      SSLVPN-VIF0 to up [OK]
*Aug  7 05:14:11.320: GLOBAL: adj mgr notified of fibidb state change int
                      FastEthernet0/0 to up [OK]
*Aug  7 05:14:11.320: GLOBAL: adj mgr notified of fibidb state change int
                      FastEthernet0/1 to up [OK]
*Aug  7 05:14:11.324: GLOBAL: adj mgr notified of fibidb state change int
*Aug  7 05:14:11.324: GLOBAL: adj mgr notified of fibidb state change int
                      Serial3/1 to up [OK]
*Aug  7 05:14:12.064: GLOBAL: adj mgr notified of fibidb state change int
                      Serial3/0 to down [OK]
*Aug  7 05:14:12.080: GLOBAL: adj mgr notified of fibidb state change int
                      Serial3/1 to down [OK]
*Aug  7 05:14:17.292: GLOBAL: adj ipv4 bundle changed to IPv4 no fixup adj oce [OK]
*Aug  7 05:14:17.292: ADJ: IP 10.4.9.1 FastEthernet0/0: update oce bundle,  IPv4
                       incomplete adj oce [OK]
*Aug  7 05:14:17.292: ADJ: IP 10.4.9.1 FastEthernet0/0: allocate [OK]
*Aug  7 05:14:17.292: ADJ: IP 10.4.9.1 FastEthernet0/0: request resolution [OK]
*Aug  7 09:10:25.576: ADJ: IP 10.4.9.1 FastEthernet0/0: request to add ARP [OK]
*Aug  7 09:10:25.576: ADJ: IP 10.4.9.1 FastEthernet0/0: allocate [Ignr]
*Aug  7 09:10:25.576: ADJ: IP 10.4.9.1 FastEthernet0/0: add source ARP [OK]
*Aug  7 09:10:25.580: ADJ: IP 10.4.9.1 FastEthernet0/0: request to update [OK]
*Aug  7 09:10:25.580: ADJ: IP 10.4.9.1 FastEthernet0/0: update oce bundle,  IPv4
                       no fixup adj oce [OK]
*Aug  7 09:10:25.580: ADJ: IP 10.4.9.1 FastEthernet0/0: update [OK]      IPv4 no
 fixup adj oce [OK]
*Aug  7 05:14:11.324: GLOBAL: adj mgr notified of fibidb state change int
                      Serial3/1 to up [OK]
*Aug  7 05:14:12.064: GLOBAL: adj mgr notified of fibidb state change int
                      Serial3/0 to down [OK]
*Aug  7 05:14:12.080: GLOBAL: adj mgr notified of fibidb state change int
                      Serial3/1 to down [OK]
*Aug  7 05:14:17.292: GLOBAL: adj ipv4 bundle changed to IPv4 no fixup adj oce [OK]
*Aug  7 05:14:17.292: ADJ: IP 10.4.9.1 FastEthernet0/0: update oce bundle,  IPv4
                       incomplete adj oce [OK]
*Aug  7 05:14:17.292: ADJ: IP 10.4.9.1 FastEthernet0/0: allocate [OK]
*Aug  7 05:14:17.292: ADJ: IP 10.4.9.1 FastEthernet0/0: request resolution [OK]
*Aug  7 09:10:25.576: ADJ: IP 10.4.9.1 FastEthernet0/0: request to add ARP [OK]
```

```
*Aug  7 09:10:25.576: ADJ: IP 10.4.9.1 FastEthernet0/0: allocate [Ignr]
*Aug  7 09:10:25.576: ADJ: IP 10.4.9.1 FastEthernet0/0: add source ARP [OK]
*Aug  7 09:10:25.580: ADJ: IP 10.4.9.1 FastEthernet0/0: request to update [OK]
*Aug  7 09:10:25.580: ADJ: IP 10.4.9.1 FastEthernet0/0: update oce bundle,  IPv4
                      no fixup adj oce [OK]
*Aug  7 09:10:25.580: ADJ: IP 10.4.9.1 FastEthernet0/0: update [OK]
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show monitor event-trace cef

To display event trace messages for Cisco Express Forwarding, use the **show monitor event-trace cef**command in privileged EXEC mode.

show monitor event-trace cef {**all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** [*seconds*] **[detail]**| **latest [detail]**| **merged** {**all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** [*seconds*] **[detail]**| **latest [detail]**}}

Syntax Description

all	Displays all event trace messages currently in memory for Cisco Express Forwarding.
detail	(Optional) Displays detailed trace information.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
minutes	Specifies the time argument in minutes. The time argument is specified in minutes format (mmm).
hours **:** *minutes*	Specifies the time argument in hours and minutes. The time argument is specified in hours and minutes format (hh:mm).
clock	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
day month	(Optional) The day of the month from 1 to 31 and the month of the year.
from-boot	Displays event trace messages starting after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace cef from-boot ?** command.
seconds	(Optional) Displays event trace messages starting from a specified number of seconds after booting (uptime). Range: 0 to 3369.
latest	Displays only the event trace messages since the last **show monitor event-trace cef**command was entered.
merged	Displays entries in all event traces sorted by time.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show monitor event-trace cef**command to display trace message information for Cisco Express Forwarding.

The trace function is not locked while information is displayed to the console, which means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace cef**command generates a message indicating that some messages might be lost; however, messages continue to display on the console. If the number of lost messages is excessive, the **show monitor event-trace cef**command stops displaying messages.

Examples

The following is sample output from the **show monitor event-trace cef all**command:

```
Router# show monitor event-trace cef all
cef_events:
*Aug 22 20:14:58.999: SubSys  ipv4fib_ios_def_cap init
*Aug 22 20:14:58.999: SubSys  ipv6fib_ios_def_cap init
*Aug 22 20:14:58.999: Inst    unknown -> RP
*Aug 22 20:14:58.999: SubSys  fib_ios_chain init
*Aug 22 20:14:59.075: SubSys  fib_init
*Aug 22 20:14:59.075: SubSys  ipv4fib init
*Aug 22 20:14:59.075: SubSys  fib_ios init
*Aug 22 20:14:59.075: SubSys  fib_ios_if init
*Aug 22 20:14:59.075: SubSys  ipv4fib_ios init
*Aug 22 20:14:59.075: Flag    Common CEF enabled set to yes
*Aug 22 20:14:59.075: Flag    IPv4 CEF enabled set to yes
*Aug 22 20:14:59.075: Flag    IPv4 CEF switching enabled set to yes
*Aug 22 20:14:59.075: GState  CEF enabled
*Aug 22 20:14:59.075: SubSys  ipv6fib_ios init
*Aug 22 20:14:59.075: SubSys  ipv4fib_util init
*Aug 22 20:14:59.075: SubSys  ipv4fib_les init
*Aug 22 20:15:02.907: Process Background created
*Aug 22 20:15:02.907: Flag    IPv4 CEF running set to yes
*Aug 22 20:15:02.907: Process Background event loop enter
*Aug 22 20:15:02.927: Flag    IPv4 CEF switching running set to yes

cef_interface:
*Aug 22 20:14:58.999: Et0/0        (hw  3) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et0/1        (hw  4) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et0/2        (hw  5) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et0/3        (hw  6) SWvecLES <unknown> (0x01096A3C)
```

```
*Aug 22 20:14:58.999: Et1/0        (hw  7) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et1/1        (hw  8) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et1/2        (hw  9) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et1/3        (hw 10) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Se2/0        (hw 11) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Se2/1        (hw 12) SWvecLES <unknown> (0x01096A3C)
.
.
.
```

The output is in table format where the first column contains a timestamp, the second column lists the type of event, and the third column lists the detail for the event.

The table below describes the significant fields shown in the display.

Table 22: show monitor event -trace cef all Field Descriptions

Field	Description
*Aug 22 20:14:58.999:	A timestamp that indicates the month, day, and time when the event was captured.
cef_events	Indicates that messages about Cisco Express Forwarding events will follow.
SubSys	The event type that is related to the initialization of a subset of functionality. For example, "ipv4fib_ios_def_cap init" is the initialization of IPv4 Cisco Express Forwarding IOS default capabilities.
Inst	The event type that records changes to an instance, such as changes to a Route Processor (RP) or line card. For example, a change from unknown to RP occurs at startup when the software detects what the instance is.
Flag	The event type that records changes to Cisco Express Forwarding control flags that handle what is running, for example, "Common CEF enabled set to yes".
GState	The event type that notes changes to the Cisco Express Forwarding global state: "CEF enabled" or "CEF disabled".
Process	The event type that records when Cisco Express Forwarding processes are created, begin, or complete normal operations,
cef_interface	Indicates that messages about Cisco Express Forwarding interface events will follow.
Et0/0	Indicates that the following recorded event affects interface Ethernet 0/0.

Field	Description
(hw 3) SWvecLES <unknown> (0x01096A3C)	The detail for this event is as follows: • (hw3)--The hardware interface descriptor block (idb) number for the interface • SWvecLES--The switching vector for this interface is changed to the LES path • <unknown>--The switching vector name is unknown • (0x01096A3C)--The address in memory of the switching vector

The following is sample output from the **show monitor event-trace cef latest** command:

```
Router# show monitor event-trace cef latest
cef_events:
cef_interface:
*Aug 22 20:14:59.075: Se3/0        (sw 15) FlagCha  0x60C1 add puntLC
*Aug 22 20:14:59.075: <empty>      (hw 16) State    down -> up
*Aug 22 20:14:59.075: <empty>      (hw 16) Create   new
*Aug 22 20:14:59.075: Se3/1        (hw 16) NameSet
*Aug 22 20:14:59.075: Se3/1        (hw 16) HWIDBLnk Serial3/1(16)
*Aug 22 20:14:59.075: Se3/1        (hw 16) RCFlags  None -> Fast
*Aug 22 20:14:59.075: <empty>      (sw 16) VRFLink  IPv4:id0 - success
*Aug 22 20:14:59.075: <empty>      (sw 16) State    deleted -> down
*Aug 22 20:14:59.075: <empty>      (sw 16) Create   new
*Aug 22 20:14:59.075: Se3/1        (sw 16) NameSet
*Aug 22 20:14:59.075: Se3/1        (sw 16) FIBHWLnk Serial3/1(16)
*Aug 22 20:14:59.075: Se3/1        (sw 16) SWIDBLnk Serial3/1(16)
*Aug 22 20:14:59.075: Se3/1        (sw 16) FlagCha  0x6001 add p2p|input|first
*Aug 22 20:14:59.075: Se3/1        (sw 16) FlagCha  0x6041 add auto_adj
*Aug 22 20:14:59.075: Se3/1        (sw 16) Impared  lc rea Queueing configuration
*Aug 22 20:14:59.075: Se3/1        (sw 16) FlagCha  0x60C1 add puntLC
*Aug 22 20:14:59.075: <empty>      (hw 17) State    down -> up
*Aug 22 20:14:59.075: <empty>      (hw 17) Create   new
*Aug 22 20:14:59.075: Se3/2        (hw 17) NameSet
```

The table below describes the significant fields shown in the display.

Table 23: show monitor event-trace cef latest Field Descriptions

Field	Description
(sw15) FlagCha 0x60C1 add puntLC	The detail for this event is as follows: • (sw 15)--The software idb number for the interface. • FlagCha--Indicates a Forwarding Information Base interface descriptor block (fibidb) flag change for the interface. • 0x60C1--The flag field in hexadecimals after the change. • add--Flags are added. • puntLC--Changed flag or flags--puntLC is one flag that indicates packets that are switched to this interface on the linecard are handled by the next slower path (not switched by Cisco Express Forwarding).
State	Indicates a change in state, for example when an interface goes from an up state to a down state.
Create	Indicates that an interface was created.
Nameset	Indicates that the name of the interface changed.
RCFlags	Indicates that a route cache change occured.

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.
monitor event-trace cef ipv6 (global)	Configures event tracing for Cisco Express Forwarding IPv6 events.
show monitor event-trace cef events	Displays event trace messages for Cisco Express Forwarding events.

Command	Description
show monitor event-trace cef interface	Displays event trace messages for Cisco Express Forwarding interface events.
show monitor event-trace cef ipv4	Displays event trace messages for Cisco Express Forwarding IPv4 events.
show monitor event-trace cef ipv6	Displays event trace messages for Cisco Express Forwarding IPv6 events.

show monitor event-trace cef events

To display event trace messages for Cisco Express Forwarding events, use the **show monitor event-trace cef events**command in privileged EXEC mode.

show monitor event-trace cef events {**all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** [*seconds*] **[detail]**| **latest [detail]**| **parameters**}

Syntax Description

all	Displays all event trace messages currently in memory for Cisco Express Forwarding.
detail	(Optional) Displays detailed trace information.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
minutes	Time argument (mmm) in minutes.
hours **:** *minutes*	Time argument (hh:mm) in hours and minutes. You must enter the colon (:) in the argument.
clock	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
day month	(Optional) The day of the month from 1 to 31 and the name of the month of the year.
from-boot	Displays event trace messages starting after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace cef from-boot ?** command.
seconds	(Optional) Displays event trace messages starting from a specified number of seconds after booting (uptime). Range: 0 to 3279.
latest	Displays only the event trace messages generated since the last **show monitor event-trace cef**command was entered.
parameters	Displays parameters configured for the trace. The only parameter displayed is the size (number of trace messages) of the trace file.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show monitor event-trace cef events** command to display trace message information about events associated with Cisco Express Forwarding.

The trace function is not locked while information is being displayed to the console. This means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace cef events**command generates a message indicating that some messages might be lost; however, messages continue to be displayed on the console. If the number of lost message is excessive, the **show monitor event-trace cef events**command stops displaying messages.

Examples

The following is sample output from the **show monitor event-trace cef events all**command:

```
Router# show monitor event-trace cef events all
*Aug 13 17:38:27.999: SubSys  ipv4fib_ios_def_cap init
*Aug 13 17:38:27.999: SubSys  ipv6fib_ios_def_cap init
*Aug 13 17:38:27.999: Inst    unknown -> RP
*Aug 13 17:38:27.999: SubSys  fib_ios_chain init
*Aug 13 17:38:28.199: SubSys  fib init
*Aug 13 17:38:28.199: SubSys  ipv4fib init
*Aug 13 17:38:28.199: SubSys  fib_ios init
*Aug 13 17:38:28.199: SubSys  fib_ios_if init
*Aug 13 17:38:28.199: SubSys  ipv4fib_ios init
*Aug 13 17:38:28.199: Flag    Common CEF enabled set to yes
*Aug 13 17:38:28.199: Flag    IPv4 CEF enabled set to yes
*Aug 13 17:38:28.199: Flag    IPv4 CEF switching enabled set to yes
*Aug 13 17:38:28.199: GState  CEF enabled
*Aug 13 17:38:28.199: SubSys  ipv6fib_ios init
*Aug 13 17:38:28.199: SubSys  ipv4fib_util init
*Aug 13 17:38:28.199: SubSys  ipv4fib_les init
*Aug 13 17:38:34.059: Process Background created
*Aug 13 17:38:34.059: Flag    IPv4 CEF running set to yes
*Aug 13 17:38:34.059: Process Background event loop enter
*Aug 13 17:38:34.079: Flag    IPv4 CEF switching running set to yes
```

The table below describes the significant fields shown in the display.

Table 24: show monitor event-trace cef events all Field Descriptions

Field	Description
*Aug 13 17:38:27.999:	A time stamp that indicates the month, day, and time when the event was captured.
SubSys	The event type that is related to the initialization of a subset of functionality. For example, "ipv4fib_ios_def_cap init" is the initialization of IPv4 Cisco Express Forwarding IOS default capabilities.
Inst	The event type that records changes to an instance, such as changes to a Route Processor (RP) or line card. For example, a change from unknown to RP occurs at startup when the software detects what the instance is.
Flag	The event type that records changes to Cisco Express Forwarding control flags that handle what is running, for example, "Common CEF enabled set to yes".
GState	The event type that notes changes to the Cisco Express Forwarding global state: "CEF enabled" or "CEF disabled".
Process	The event type that records when Cisco Express Forwarding processes are created, begin, or complete normal operations,

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.
monitor event-trace cef ipv6 (global)	Configures event tracing for Cisco Express Forwarding IPv6 events.
show monitor event-trace cef	Displays event trace messages for Cisco Express Forwarding.

Command	Description
show monitor event-trace cef interface	Displays event trace messages for Cisco Express Forwarding interface events.
show monitor event-trace cef ipv4	Displays event trace messages for Cisco Express Forwarding IPv4 events.
show monitor event-trace cef ipv6	Displays event trace messages for Cisco Express Forwarding IPv6 events.

show monitor event-trace cef interface

To display event trace messages for Cisco Express Forwarding interface events, use the **show monitor event-trace cef interface**command in privileged EXEC mode

show monitor event-trace cef interface {**all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** [*seconds*] **[detail]**| **latest [detail]**| **parameters**| {**hw**| **sw**} *interface-index* {**all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** [*seconds*] **[detail]**| **latest [detail]**}}

Syntax Description

all	Displays all event trace messages currently in memory for Cisco Express Forwarding.
detail	(Optional) Displays detailed trace information for Cisco Express Forwarding interface events.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
minutes	Time argument (mmm) in minutes.
hours **:** *minutes*	Time argument (hh:mm) in hours and minutes. You must enter the colon (:) in the argument.
clock	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
day month	(Optional) The day of the month from 1 to 31 and the name of the month of the year.
from-boot	Displays event trace messages starting after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace cef from-boot ?** command.
seconds	(Optional) Displays event trace messages starting from a specified number of seconds after booting (uptime). Range: 0 to 4429.
latest	Displays only the event trace messages generated since the last **show monitor event-trace cef**command was entered.
parameter	Displays parameters configured for the trace.

hw	Displays trace events for the specified hardware interface index.
sw	Displays trace events for the specified hardware interface index
interface-index	Specifies the interface index. Range: 0 to 10000.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show monitor event-trace cef interface** to display trace message information about interface events associated with Cisco Express Forwarding.

The trace function is not locked while information is displayed to the console. This means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace cef interface**command generates a message indicating that some messages might be lost; however, messages continue to be displayed on the console. If the number of lost messages is excessive, the **show monitor event-trace cef interface**command stops displaying messages.

Examples

The following is sample output from the **show monitor event-trace cef interface latest** command:

```
Router# show monitor event-trace cef interface latest
*Aug 22 20:14:58.999: Et0/0        (hw  3) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et0/1        (hw  4) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et0/2        (hw  5) SWvecLES <unknown> (0x01096A3C)
*Aug 22 20:14:58.999: Et0/3        (hw  6) SWvecLES <unknown> (0x01096A3C)
.
.
.
*Aug 22 20:14:59.075: <empty>      (hw  3) State    down -> up
*Aug 22 20:14:59.075: <empty>      (hw  3) Create   new
*Aug 22 20:14:59.075: Et0/0        (hw  3) NameSet
*Aug 22 20:14:59.075: Et0/0        (hw  3) HWIDBLnk Ethernet0/0(3)
*Aug 22 20:14:59.075: Et0/0        (hw  3) RCFlags  None -> Fast
*Aug 22 20:14:59.075: <empty>      (sw  3) VRFLink  IPv4:id0 - success
```

```
*Aug 22 20:14:59.075: <empty>      (sw  3) State    deleted -> down
*Aug 22 20:14:59.075: <empty>      (sw  3) Create   new
*Aug 22 20:14:59.075: Et0/0        (sw  3) NameSet
*Aug 22 20:14:59.075: Et0/0        (sw  3) FIBHWLnk Ethernet0/0(3)
*Aug 22 20:14:59.075: Et0/0        (sw  3) SWIDBLnk Ethernet0/0(3)
*Aug 22 20:14:59.075: Et0/0        (sw  3) FlagCha  0x6000 add input|first
*Aug 22 20:14:59.075: Et0/0        (sw  3) State    down -> up
*Aug 22 20:14:59.075: <empty>      (hw  4) State    down -> up
*Aug 22 20:14:59.075: <empty>      (hw  4) Create   new
*Aug 22 20:14:59.075: Et0/1        (hw  4) NameSet
*Aug 22 20:14:59.075: Et0/1        (hw  4) HWIDBLnk Ethernet0/1(4)
*Aug 22 20:14:59.075: Et0/1        (hw  4) RCFlags  None -> Fast
*Aug 22 20:14:59.075: <empty>      (sw  4) VRFLink  IPv4:id0 - success
*Aug 22 20:14:59.075: <empty>      (sw  4) State    deleted -> down
*Aug 22 20:14:59.075: <empty>      (sw  4) Create   new
*Aug 22 20:14:59.075: Et0/1        (sw  4) NameSet
*Aug 22 20:14:59.075: Et0/1        (sw  4) FIBHWLnk Ethernet0/1(4)
*Aug 22 20:14:59.075: Et0/1        (sw  4) SWIDBLnk Ethernet0/1(4)
*Aug 22 20:14:59.075: Et0/1        (sw  4) FlagCha  0x6000 add input|first
*Aug 22 20:14:59.075: Et0/1        (sw  4) State    down -> up
.
.
.
```

The table below describes the significant fields shown in the display.

Table 25: show monitor event-trace cef interface latest Field Descriptions

Field	Description
Et0/0	Indicates that the following recorded event affects interface Ethernet 0/0.
(hw3) SWvecLES <unknown> (0x01096A3C)	The detail for this event is as follows: • (hw3)--The hardware interface descriptor block (idb) number for the interface • SWvecLES--The switching vector for this interface is changed to the LES path • <unknown>--The switching vector name is unknown • (0x01096A3C)--The address in memory of the switching vector
State	Indicates a change in state, for example, when an interface goes from the up state to the down state.
Create	Indicates that an interface was created.
Nameset	Indicates that the name of the interface changed.
RCFlags	Indicates that a route cache change occurred.
FlagCha	Indicates that a Forwarding Information Base interface descriptor block (fibidb) flag changed for the interface.

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.
monitor event-trace cef ipv6 (global)	Configures event tracing for Cisco Express Forwarding IPv6 events.
show monitor event-trace cef	Displays event trace messages for Cisco Express Forwarding.
show monitor event-trace cef events	Displays event trace messages for Cisco Express Forwarding events.
show monitor event-trace cef ipv4	Displays event trace messages for Cisco Express Forwarding IPv4 events.
show monitor event-trace cef ipv6	Displays event trace messages for Cisco Express Forwarding IPv6 events.

show monitor event-trace cef ipv4

To display event trace messages for Cisco Express Forwarding IPv4 events, use the **show monitor event-trace cef ipv4**command in privileged EXEC mode.

show monitor event-trace cef ipv4 {{*ip-address*| **vrf** *vrf-name ip-address*} {**all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** *seconds* **[detail]**| **latest [detail]**}| **all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** *seconds* **[detail]**| **latest [detail]**| **parameters**}

Syntax Description

ip-address	Specifies an IP address of interest in A.B.C.D format.
vrf *vrf-name*	Specifies a Cisco Express Forwarding IPv4 Virtual Private Network (VPN) routing and Forwarding (VRF) table. The *vrf-name* argument specifies the name of the VRF of interest.
all	Displays all event trace messages currently in memory for Cisco Express Forwarding IPv4 events.
detail	(Optional) Displays detailed trace information for Cisco Express Forwarding IPv4 events.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
minutes	Time argument (mmm) in minutes.
hours **:** *minutes*	Time argument (hh:mm) in hours and minutes. You must enter the colon (:) in the argument.
clock	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
day month	(Optional) The day of the month from 1 to 31 and the name of the month of the year.
from-boot	Displays event trace messages starting after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace cef from-boot ?** command.
seconds	(Optional) Displays event trace messages starting from a specified number of seconds after booting (uptime). Range: 0 to 3279.

latest	Displays only the event trace messages generated since the last **show monitor event-trace cef ipv4**command was entered.
parameters	Displays parameters configured for the trace.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show monitor event-trace cef ipv4** command to display trace message information for Cisco Express Forwarding IPv4 events.

The trace function is not locked while information is displayed to the console. This means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace cef ipv4**command generates a message indicating that some messages might be lost; however, messages continue to be displayed on the console. If the number of lost messages is excessive, the **show monitor event-trace cef ipv4**command stops displaying messages.

Examples

The following is sample output from the **show monitor event-trace cef ipv4 all**command:

```
Router# show monitor event-trace cef ipv4 all
*Aug 22 20:14:59.075:  [Default] *.*.*.*/*             Allocated FIB table
                      [OK]
*Aug 22 20:14:59.075:  [Default] *.*.*.*/*'00          Add source Default table
                      [OK]
*Aug 22 20:14:59.075:  [Default] 0.0.0.0/0'00          FIB add src DRH (ins)
                      [OK]
*Aug 22 20:14:59.075:  [Default] *.*.*.*/*'00          New FIB table
                      [OK]
*Aug 22 20:15:02.927:  [Default] *.*.*.*/*'00          FIB refresh start
                      [OK]
.
.
.
```

The table below describes the significant fields shown in the display.

Table 26: show monitor event-trace cef ipv4 all Field Descriptions

Field	Description
*Aug 22 20:14:59.075:	Time stamp that indicates the month, day, and time when the event was captured.
[Default] *.*.*.*/*	Identifies the default VRF.
Allocated FIB table [OK]	Provides the event detail and indicates if the event happened or if it was ignored ([Ignr]). In this instance, a FIB table was allocated.
Add source Default table	Indicates that a source for the Default table was added.

Following is sample output from the **show monitor event-trace cef ipv4 parameters** command:

```
Router# show monitor event-trace cef ipv4 parameters
Trace has 1000 entries
Stacktrace is disabled by default
Matching all events
```

The table below describes the significant fields shown in the display.

Table 27: show monitor event-trace cef ipv4 parameters Field Descriptions

Field	Description
Trace has 1000 entries	The size of the event logging buffer is 1000 entries.
Stacktrace is disabled by default	Stack trace at tracepoints is disabled.
Matching all events	Event tracing for all events is matched.

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.
monitor event-trace cef ipv6 (global)	Configures event tracing for Cisco Express Forwarding IPv6 events.

Command	Description
show monitor event-trace cef	Displays event trace messages for Cisco Express Forwarding.
show monitor event-trace cef events	Displays event trace messages for Cisco Express Forwarding events.
show monitor event-trace cef interface	Displays event trace messages for Cisco Express Forwarding interface events.
show monitor event-trace cef ipv6	Displays event trace messages for Cisco Express Forwarding IPv6 events.

show monitor event-trace cef ipv6

To display event trace messages for Cisco Express Forwarding IPv6 events, use the **show monitor event-trace cef ipv6**command in privileged EXEC mode.

show monitor event-trace cef ipv6 {*ipv6-address* {**all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** *seconds* **[detail]**| **latest [detail]**}| **all [detail]**| **back** {*minutes*| *hours* **:** *minutes*} **[detail]**| **clock** *hours* **:** *minutes* [*day month*] **[detail]**| **from-boot** *seconds* **[detail]**| **latest [detail]**| **parameters**}

Syntax Description

ipv6-address	Specifies an IPv6 address. This address must be specified in hexadecimals using 16-bit values between colons, as specified in RFC 2373.
all	Displays all event trace messages currently in memory for Cisco Express Forwarding IPv6 events.
detail	(Optional) Displays detailed trace information for Cisco Express Forwarding IPv6 events.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
minutes	Time argument (mmm) in minutes.
hours **:** *minutes*	Time argument (hh:mm) in hours and minutes. You must enter the colon (:) in the argument.
clock	Displays event trace messages starting from a specific clock time in hours and minutes format (hh:mm).
day month	(Optional) The day of the month from 1 to 31 and the name of the month of the year.
from-boot	Displays event trace messages starting after booting (uptime). To display the uptime, in seconds, enter the **show monitor event-trace cef from-boot ?** command.
seconds	(Optional) Displays event trace messages starting from a specified number of seconds after booting (uptime). Range: 0 to 3279.
latest	Displays only the event trace messages generated since the last **show monitor event-trace cef ipv6**command was entered.

parameters	Displays parameters configured for the trace.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show monitor event-trace cef ipv6** command to display trace message information for Cisco Express Forwarding IPv6 events.

The trace function is not locked while information is displayed to the console. This means that new trace messages can accumulate in memory. If entries accumulate faster than they can be displayed, some messages can be lost. If this happens, the **show monitor event-trace cef ipv6**command generates a message indicating that some messages might be lost; however, messages continue to be displayed on the console. If the number of lost messages is excessive, the **show monitor event-trace cef ipv6**command stops displaying messages.

Examples

The following is a sample of the **show monitor event-trace cef ipv6 all** command:

```
Router# show monitor event-trace cef ipv6 all

*Aug 22 20:14:59.075:  [Default] *::*/*                Allocated FIB table
                      [OK]
*Aug 22 20:14:59.075:  [Default] *::*/*'00             Add source Default table
                      [OK]
*Aug 22 20:14:59.075:  [Default] ::/0'00               FIB add src DRH (ins)
                      [OK]
*Aug 22 20:14:59.075:  [Default] *::*/*'00             New FIB table
                      [OK]
```

The table below describes the significant fields shown in the display.

Table 28: show monitor event-trace cef ipv6 all Field Descriptions

Field	Description
*Aug 22 20:14:59.075:	Time stamp that indicates the month, day, and time when the event was captured.

Field	Description
[Default] *::*/*	Identifies the default VRF.
Allocated FIB table [OK]	Provides the event detail and indicates if the event happened. In this instance, a FIB table was allocated.

The following is sample output from the **show monitor event-trace cef ipv6 parameters** command:

```
Router# show monitor event-trace cef ipv6 parameters
Trace has 1000 entries
Stacktrace is disabled by default
Matching all events
```

The table below describes the significant fields shown in the display.

Table 29: show monitor event-trace cef ipv6 parameters Field Descriptions

Field	Description
Trace has 1000 entries	The size of the event logging buffer is 1000 entries.
Stacktrace is disabled by default	Stack trace at tracepoints is disabled.
Matching all events	Event tracing for all events is matched.

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.
monitor event-trace cef ipv6 (global)	Configures event tracing for Cisco Express Forwarding IPv6 events.
show monitor event-trace cef	Displays event trace messages for Cisco Express Forwarding.
show monitor event-trace cef events	Displays event trace messages for Cisco Express Forwarding events.
show monitor event-trace cef interface	Displays event trace messages for Cisco Express Forwarding interface events.

Command	Description
show monitor event-trace cef ipv4	Displays event trace messages for Cisco Express Forwarding IPv4 events.

show monitor event-trace continuous

To display event trace messages of components that have enabled continuous display, use the **show monitor event-trace continuous** command in privileged EXEC mode.

show monitor event-trace continuous

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show monitor event-trace continuous** command. The fields are self-explanatory.

```
Router# show monitor event-trace continuous

Event trace continuous display enabled for:
datainteg
tunnel
adjacency
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.

Command	Description
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show monitor event-trace cpu-report

To display event trace messages for the CPU, use the **show monitor event-trace cpu-report**command in user EXEC or privileged EXEC mode.

show monitor event-trace cpu-report {**brief** {**all**| **back** {*mmm*| *hhh* **:** *mm*}| **clock** *hh* **:** *mm* [*date month*| *month date*]| **from-boot** [*seconds*]| **latest**} **[detail]**| **handle** *handle-number*}

Syntax Description

brief	Displays a brief CPU report.
all	Displays all event trace messages currently in memory for the CPU.
back	Specifies how far back from the current time you want to view messages. For example, you can gather messages from the last 30 minutes.
{*mmm* | *hhh* **:** *mm*}	Duration of the trace. The format is mmm or hhh:mm.
clock	Displays event trace messages starting from a specific clock time.
hh **:** *mm*	Integer value that is the length of time, in hours and minutes. The format is hh:mm.
date	(Optional) Day of the month (from 1 to 31).
month	(Optional) Displays the month of the year.
from-boot	Displays event trace messages starting from a specified number of seconds after booting.
seconds	(Optional) Number of seconds since the networking device was last booted (uptime).
latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
detail	(Optional) Displays detailed event trace information.
handle	Displays a detailed CPU report for a specified handle number.
handle-number	Handle number. Valid values are from 1 to 255.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show monitor event-trace cpu-report** command with the **brief** keyword to display the CPU report details. To display individual snapshots, use the **show monitor event-trace cpu-report handle** *handle-number* command.

To display the uptime, in seconds, enter the **show monitor event-trace cpu-report from-boot ?** command.

Examples

To display CPU report details for event tracing on a networking device, enter the **show monitor event-trace cpu-report brief all** command. The field descriptions are self-explanatory.

```
Router# show monitor event-trace cpu-report brief all
Timestamp   : Handle Name               Description
00:01:07.320:  1     CPU                None
```

To display CPU report details for event tracing on a networking device for the handle number 1, enter the **show monitor event-trace cpu-report handle 1** command. The field descriptions are self-explanatory.

```
Router# show monitor event-trace cpu-report handle 1
00:01:07.320:  1     CPU                None
################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 21:03:56
Queue Statistics
----------------
             Exec Count  Total CPU    Response Time        Queue Length
                                        (avg/max)             (avg/max)
Critical           1          0          0/0                   1/1
High               5          0          0/0                   1/1
Normal           178          0          0/0                   2/9
Low               15          0          0/0                   2/3
Common Process Information
------------------------------
 PID Name            Prio Style
------------------------------
  10 AAA high-capacit M  New
 133 RADIUS TEST CMD  M  New
  47 VNM DSPRM MAIN   H  New
  58 TurboACL         M  New
  97 IP Background    M  New
  99 CEF: IPv4 proces L  New
 112 X.25 Background  M  New
 117 LFDp Input Proc  M  New
   3 Init             M  Old
```

```
CPU Intensive processes
--------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
--------------------------------------------------------------------------------
   3   820          6   136/236         1     24/24              18  887/15172
Priority Suspends
-----------------------------------
 PID Exec Count Prio-Susps
-----------------------------------
   3          6          1
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
  10          1 15192/15192
 133          1 15192/15192
  58          1 15192/15192
 112          1 15192/15192
 117          1 15192/15192
  99          1 15172/15172
  47          1 15172/15172
  97          1 15172/15172
################################################################################
Global Statistics
-----------------
5 sec CPU util 0%/0% Timestamp 00:00:00
Queue Statistics
----------------
        Exec Count  Total CPU     Response Time           Queue Length
                                     (avg/max)               (avg/max)
Critical      0          0             0/0                    0/0
High          0          0             0/0                    0/0
Normal        0          0             0/0                    0/0
Low           0          0             0/0                    0/0

Common Process Information
------------------------------
 PID Name            Prio Style
------------------------------
CPU Intensive processes
--------------------------------------------------------------------------------
 PID Total       Exec    Quant         Burst  Burst size  Schedcall  Schedcall
     CPUms      Count   avg/max        Count avg/max(ms)      Count Per avg/max
--------------------------------------------------------------------------------
Priority Suspends
-----------------------------------
 PID Exec Count Prio-Susps
-----------------------------------
Latencies
-------------------------
 PID Exec Count   Latency
                  avg/max
-------------------------
################################################################################
```

Related Commands

Command	Description
monitor event-trace cpu-report (EXEC)	Monitors event tracing of the CPU reports.
monitor event-trace cpu-report (global)	Monitors the collection of CPU report traces.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.

show monitor event-trace hw-api

To display event trace information about the HW-API events, use the **show monitor event-trace hw-api**command in privileged EXEC mode.

show monitor event-trace hw-api {{**all**| **back** *time*| **clock** *time day month*| **from-boot** [*time*]| **latest**} **[detail]**| **parameters**}

Syntax Description

all	Displays all event traces in the current buffer.
back	Displays trace from a specific time far back in the past.
time	Duration of trace in the format mmm or hhh:mm.
clock	Displays trace from a specific clock time and date.
time	Time in the format hh:mm.
day	Day of the month.
month	Month of the year.
from-boot	Displays trace from specified seconds after booting.
time	(Optional) Time after boot in seconds. Valid range is 0 to 217696.
latest	Displays latest trace events since last display.
detail	(Optional) Displays detailed trace information.
parameters	Displays the parameters of the trace.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(17)T	This command was introduced.
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.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following is sample output from the **show monitor event-trace hw-api all** command. The fields are self-explanatory.

```
Router# show monitor event-trace hw-api all
*Jan 14 17:42:25.207: bwalk at 000756FC adj Et0/0 IP 192.168.1.1 0
                           0.000
*Jan 14 17:42:25.207: bwalk as 00075600 adj Et0/0 IP 192.168.1.1 0
                           0.000
*Jan 14 17:42:25.207: bwalk at 000756FC adj Et0/0 IP 192.168.1.1 0
                           0.000
*Jan 14 17:42:25.207: bwalk as 00075600 rpflst                          014B1450
                           0.000
*Jan 14 17:42:25.207: bwalk at 000756FC rpflst                          014B1450
                           0.000
*Jan 14 17:42:25.207: bwalk as 00075600 fibidb Ethernet0/0
                           0.000
*Jan 14 17:42:25.207: bwalk at 000756FC fibidb Ethernet0/0
                           0.000
*Jan 14 17:42:25.207: bwalk as 00075600 adj Et0/0 IP 192.168.1.1 0
                           0.000
*Jan 14 17:42:25.207: bwalk at 000756FC adj Et0/0 IP 192.168.1.1 0
                           0.000
*Jan 14 17:42:25.207: bwalk as 00075600 rpflst                          014B1450
                           0.000
*Jan 14 17:42:25.207: bwalk at 000756FC rpflst                          014B1450
                           0.000
*Jan 14 17:42:25.207: bwalk as 00075600 adj Et0/0 IP 192.168.1.1 0
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.
monitor event-trace hw-api	Monitors control even tracing of HW-API events.

show monitor event-trace merged-list

To display event trace information for a list of trace buffers sorted by time, use the **show monitor event-trace merged-list**command in privileged EXEC mode.

show monitor event-trace merged-list *trace-buffer-name1* [... [*trace-buffer-name4*]]

Syntax Description

trace-buffer-name	Name of the trace buffer. You can specify up to four trace buffers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show monitor event-trace merged-list** command. The output displays event trace information for the lists cef_interface and licnvram, sorted by time. The fields are self-explanatory.

```
Router# show monitor event-trace merged-list list1 cef_interface licnvram
*Dec  7 14:02:21.019: licnvram: **NVRAM: Original config magic is good
*Dec  7 14:02:21.019: licnvram: **NVRAM: Backup config magic is good
*Dec  7 14:02:21.019: licnvram: **NVRAM: Second Backup Magic is not good
*Dec  7 14:02:42.767: cef_interface: Gi0/0        (hw  2) SWvecLES Null
                                     (0x622026C8)
*Dec  7 14:02:42.767: cef_interface: Gi0/1        (hw  3) SWvecLES Null
                                     (0x622026C8)
*Dec  7 14:02:42.767: cef_interface: AO1/0        (hw  5) SWvecLES Null
                                     (0x622026C8)
*Dec  7 14:02:42.767: cef_interface: In2/0        (hw  6) SWvecLES Null
                                     (0x622026C8)
*Dec  7 14:02:42.767: cef_interface: Vo0          (hw  4) SWvecLES Null
                                     (0x622026C8)
*Dec  7 14:02:42.851: cef_interface: <empty>      (hw  2) Create   new ['0]
*Dec  7 14:02:42.851: cef_interface: <empty>      (hw  2) State    down -> up
```

```
*Dec  7 14:02:42.851: cef_interface: Gi0/0        (hw  2) NameSet
*Dec  7 14:02:42.851: cef_interface: Gi0/0        (hw  2) HWIDBLnk GigabitEthernet
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls event trace functions for a specified Cisco IOS software subsystem component.
monitor event-trace (global)	Configures event tracing for a specified Cisco IOS software subsystem component.
monitor event-trace dump-traces	Saves trace messages for all event traces currently enabled on the networking device.