



Cisco IOS IP Switching Command Reference

November 2010

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS IP Switching Command Reference

© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Introduction ISW-1

IP Switching Commands ISW-3

- cef table consistency-check ISW-4
- cef table download ISW-7
- cef table output-chain build ISW-9
- cef table rate-monitor-period ISW-12
- clear adjacency ISW-13
- clear adjacency epoch ISW-15
- clear cef interface ISW-16
- clear cef linecard ISW-17
- clear cef table ISW-19
- clear ip cache ISW-22
- clear ip cef epoch ISW-23
- clear ip cef epoch full ISW-25
- clear ip cef event-log ISW-27
- clear ip cef inconsistency ISW-29
- clear ip cef prefix-statistics ISW-31
- clear ip mds ISW-32
- clear ip mds forwarding ISW-34
- clear ip mds linecard ISW-35
- clear ip traffic ISW-36
- clear mls cef ip accounting per-prefix ISW-37
- clear pxf ISW-38
- ip cache-invalidate-delay ISW-40
- ip cef ISW-42
- ip cef accounting ISW-44
- ip cef linecard ipc memory ISW-46
- ip cef load-sharing algorithm ISW-47
- ip cef optimize neighbor resolution ISW-49
- ip cef table adjacency-prefix ISW-50

ip cef table adjacency-prefix	ISW-52
ip cef table consistency-check	ISW-53
ip cef table event-log	ISW-56
ip cef table resolution-timer	ISW-58
ip cef traffic-statistics	ISW-60
ip load-sharing	ISW-62
ip route-cache	ISW-64
ip route-cache policy	ISW-73
ip verify unicast notification threshold	ISW-74
ip verify unicast reverse-path	ISW-76
ip verify unicast source reachable-via	ISW-80
ip verify unicast vrf	ISW-85
ipv6 cef	ISW-87
ipv6 cef accounting	ISW-89
ipv6 cef distributed	ISW-91
ipv6 cef load-sharing algorithm	ISW-93
ipv6 cef optimize neighbor resolution	ISW-95
ipv6 verify unicast reverse-path	ISW-96
ipv6 verify unicast source reachable-via	ISW-100
mls cef maximum-routes	ISW-102
mls cef tunnel fragment	ISW-105
mls erm priority	ISW-106
mls ip	ISW-108
mls ip cef accounting per-prefix	ISW-109
mls ip cef load-sharing	ISW-110
mls ip cef rate-limit	ISW-112
mls ip cef rpf hw-enable-rpf-acl	ISW-114
mls ip cef rpf interface-group	ISW-115
mls ip cef rpf multipath	ISW-116
monitor event-trace (EXEC)	ISW-117
monitor event-trace (global)	ISW-120
monitor event-trace cef (EXEC)	ISW-123
monitor event-trace cef (global)	ISW-126
monitor event-trace cef ipv4 (global)	ISW-129
monitor event-trace cef ipv6 (global)	ISW-132

show adjacency	ISW-135
show cef	ISW-141
show cef drop	ISW-147
show cef events	ISW-149
show cef features global	ISW-151
show cef interface	ISW-153
show cef interface policy-statistics	ISW-162
show cef linecard	ISW-167
show cef memory	ISW-171
show cef not-cef-switched	ISW-174
show cef state	ISW-177
show cef subtree context client	ISW-180
show cef table	ISW-182
show cef table download priority	ISW-188
show cef timers	ISW-190
show cef vrf	ISW-192
show interface stats	ISW-194
show interfaces switching	ISW-196
show ip cache	ISW-199
show ip cef	ISW-203
show ip cef adjacency	ISW-206
show ip cef epoch	ISW-210
show ip cef events	ISW-212
show ip cef exact-route	ISW-214
show ip cef inconsistency	ISW-216
show ip cef non-recursive	ISW-218
show ip cef platform	ISW-221
show ip cef summary	ISW-223
show ip cef switching statistics	ISW-226
show ip cef traffic prefix-length	ISW-230
show ip cef tree	ISW-232
show ip cef unresolved	ISW-235
show ip cef vlan	ISW-237
show ip cef vrf	ISW-238
show ip cef with epoch	ISW-241

show ip cef with source	ISW-244
show ip mds forwarding	ISW-248
show ip mds interface	ISW-250
show ip mds stats	ISW-252
show ip mds summary	ISW-256
show ip traffic	ISW-258
show mls cef	ISW-262
show mls cef adjacency	ISW-268
show mls cef exact-route	ISW-273
show mls cef exception	ISW-274
show mls cef hardware	ISW-276
show mls cef inconsistency	ISW-279
show mls cef ip	ISW-281
show mls cef ip multicast	ISW-285
show mls cef ipv6	ISW-292
show mls cef ipx	ISW-295
show mls cef logging	ISW-296
show mls cef lookup	ISW-297
show mls cef mac	ISW-298
show mls cef maximum-routes	ISW-299
show mls cef mpls	ISW-301
show mls cef rpf	ISW-302
show mls cef statistics	ISW-304
show mls cef summary	ISW-305
show mls cef vrf	ISW-307
show mls ip cef rpf-table	ISW-309
show mls ip non-static	ISW-310
show mls ip routes	ISW-312
show mls ip static	ISW-314
show mls ip statistics	ISW-316
show mls table-contention	ISW-317
show monitor event-trace	ISW-319
show monitor event-trace adjacency	ISW-325
show monitor event-trace cef	ISW-327
show monitor event-trace cef events	ISW-331

show monitor event-trace cef interface	ISW-334
show monitor event-trace cef ipv4	ISW-337
show monitor event-trace cef ipv6	ISW-340
show monitor event-trace continuous	ISW-343
show monitor event-trace cpu-report	ISW-344
show monitor event-trace hw-api	ISW-347
show monitor event-trace merged-list	ISW-349
show pxf accounting	ISW-351
show pxf cpu access-lists	ISW-354
show pxf cpu atom	ISW-360
show pxf cpu bba	ISW-361
show pxf cpu buffers	ISW-362
show pxf cpu cef	ISW-364
show pxf cpu context	ISW-365
show pxf cpu feedback	ISW-367
show pxf cpu iedge	ISW-369
show pxf cpu ipv6	ISW-370
show pxf cpu mpls	ISW-372
show pxf cpu mroute	ISW-373
show pxf cpu pbr action	ISW-375
show pxf cpu police	ISW-379
show pxf cpu policy-data	ISW-380
show pxf cpu qos	ISW-382
show pxf cpu queue	ISW-384
show pxf cpu reasm_index	ISW-389
show pxf cpu statistics	ISW-390
show pxf cpu subblocks	ISW-396
show pxf cpu vcci	ISW-400
show pxf crash	ISW-401
show pxf dma	ISW-403
show pxf feature cef	ISW-406
show pxf feature cef vrf	ISW-407
show pxf feature nat	ISW-409
show pxf interface	ISW-410
show pxf microcode	ISW-412

show pxf netflow	ISW-414
show pxf stall-monitoring	ISW-415
show pxf statistics	ISW-418
show pxf xcm	ISW-421
show route-map ipc	ISW-424
show xdr	ISW-426
snmp mib cef throttling-interval	ISW-432
snmp-server enable traps cef	ISW-434
snmp-server host	ISW-436
switchover pxf restart	ISW-446
test cef table consistency	ISW-448



Introduction

This document describes the commands used to configure IP switching features such as Cisco Express Forwarding, Distributed Cisco Express Forwarding, and Fast Switching in Cisco IOS software.



Note

Prior to Cisco IOS Release 12.3(14)T, the commands for configuring IP switching features were presented in the *Cisco IOS Switching Services Command Reference*.

Refer to the configuration guide indicated here for configuration guidelines:

For Information About Configuring This Cisco IOS Feature...	Refer to the Following Cisco IOS Configuration Guide...
IP switching features	Cisco IOS IP Switching Configuration Guide .



IP Switching Commands

cef table consistency-check

To enable Cisco Express Forwarding table consistency checker types and parameters, use the **cef table consistency-check** command in global configuration mode. To disable consistency checkers, use the **no** form of this command.

cef table consistency-check {**ipv4** | **ipv6**} [**type** {**lc-detect** | **scan-lc-rp** | **scan-rp-lc** | **scan-rib-ios** | **scan-ios-rib**} [**count** *count-number* [**period** *seconds*] | **period** *seconds*] | **error-message** | **auto-repair** [**delay** *seconds* [**holddown** *seconds*] | **holddown** *seconds*] | **data-checking**]

no cef table consistency-check {**ipv4** | **ipv6**} [**type** {**lc-detect** | **scan-lc-rp** | **scan-rp-lc** | **scan-rib-ios** | **scan-ios-rib**} [**count** *count-number* [**period** *seconds*] | **period** *seconds*] | **error-message** | **auto-repair** | **data-checking**]

Syntax Description		
ipv4	Checks IPv4 addresses.	
ipv6	Checks IPv6 addresses.	
	Note	On the Cisco 10000 series routers, IPv6 is supported on Cisco IOS Release 12.2(28)SB and later releases.
type	(Optional) Specifies the type of consistency check to enable.	
lc-detect	(Optional) (Distributed platforms such as the Cisco 7500 series only) Detects missing prefixes on the line card. The information is confirmed by the Route Switch Processor (RSP).	
	This consistency checker operates on the line card by retrieving IP prefixes that are missing from its Forwarding Information Base (FIB) table. If IP prefixes are missing, the line card cannot forward packets for these addresses. This consistency checker then sends IP prefixes to the RSP for confirmation. If the RSP detects that it has the relevant entry, an inconsistency is detected, and an error message is displayed. Finally, the RSP sends a signal back to the line card confirming that the IP prefix is an inconsistency.	
scan-lc-rp	(Optional) (Distributed platforms only) Performs a passive scan check of tables on the line card.	
	This consistency checker operates on the line card by examining the FIB table for a configurable time period and sending the next <i>x</i> prefixes to the RSP. The RSP does an exact lookup, and if it finds the prefix missing, it reports an inconsistency. Finally, the RSP sends a signal back to the line card for confirmation.	
scan-rp-lc	(Optional) Operates on the RSP (opposite of the scan-lc-rp consistency checker) by examining the FIB table for a configurable time period and sending the next <i>x</i> prefixes to the line card.	
	The line card does an exact lookup. If it finds the prefix missing, the line card reports an inconsistency and signals the RSP for confirmation.	
scan-rib-ios	(Optional) Compares the Routing Information Base (RIB) to the FIB table and provides the number of entries missing from the FIB table.	
scan-ios-rib	(Optional) Compares the FIB table to the RIB and provides the number of entries missing from the RIB.	

count <i>count-number</i>	(Optional) Specifies the maximum number of prefixes to check per scan. The range is from 2 to 10000. The default count number is 1000 prefixes per scan for the scan-rib-ios and scan-ios-rib keywords. The default count number is 0 for the lc-detect , scan-lc-rp , and scan-rp-lc keywords.
period <i>seconds</i>	(Optional) Period between scans. Valid values are from 30 to 3600 seconds. The default is 60 seconds.
error-message	(Optional) Enables the consistency checker to generate an error message when it detects an inconsistency. By default, this function is disabled.
auto-repair	(Optional) Enables the auto repair function. By default, this function is enabled. You can enter the no form of the command to disable auto repair or enter the default form of the command to return the auto repair settings to a 10-second delay and 300-second holddown.
delay <i>seconds</i>	(Optional) Specifies how long the consistency checker waits to fix an inconsistency. The range is 10 to 300 seconds. The default delay is 10 seconds.
holddown <i>seconds</i>	(Optional) Specifies how long the consistency checker waits to reenable auto repair after auto repair runs. The range is from 300 to 3000 seconds. The default delay is 300 seconds.
data-checking	(Optional) Enables the consistency checker data-checking utility. By default, this function is disabled.

Command Default

All consistency checkers are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced. This command replaces the ip cef table consistency-check command.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Router.

Examples

The following example enables the Cisco Express Forwarding consistency checker to check IPv4 addresses:

```
Router(config)# cef table consistency-check ipv4
```

The following example enables the Cisco Express Forwarding consistency checker to check IPv4 addresses and specifies the scan-rp-lc checker to run every 60 seconds for 5000 prefixes:

```
Router(config)# cef table consistency-check ipv4 type scan-rp-lc count 5000 period 60
```

The following example enables the Cisco Express Forwarding consistency checker to check IPv4 addresses and display an error message when it finds an inconsistency:

```
Router(config)# cef table consistency-check ipv4 error-message
```

Related Commands	Command	Description
	clear cef table	Clears the Cisco Express Forwarding tables.
	clear ip cef inconsistency	Clears Cisco Express Forwarding inconsistency statistics and records found by the Cisco Express Forwarding consistency checkers.
	debug cef	Enables the display of information about Cisco Express Forwarding events.
	debug ip cef table	Enables the collection of events that affect entries in the Cisco Express Forwarding tables.
	show cef table consistency-check	Displays Cisco Express Forwarding consistency checker table values.
	show ip cef inconsistency	Displays Cisco Express Forwarding IP prefix inconsistencies.

cef table download

To set download characteristics for prefixes or routes in the Cisco Express Forwarding table, use the **cef table download** command in global configuration mode. To return to the default download characteristics, use the **no** form of this command.

cef table download { **catch-all** | **connected-route** | **default-route** | **receive-route** | **recursive-dependents** | **route-in-vrf** } **priority** *priority-number*

no cef table download { **catch-all** | **connected-route** | **default-route** | **receive-route** | **recursive-dependents** | **route-in-vrf** } **priority** *priority-number*

Syntax Description

catch-all	Any route not matched, which include Internet routes. The default priority is 4.
connected-route	Route directly connected to the router. The default priority is 2.
default-route	Default route, 0.0.0.0/0 or ::/0. The default priority is 1.
receive-route	Receive route, local address on router. The default priority is 2.
recursive-dependents	Route with recursive dependents, matches next-hop of other recursive routes. The default priority is 1.
route-in-vrf	Route in a Virtual Private Network (VPN) routing and forwarding (VRF) table. The default priority is 3.
priority	Sets the table download priority.
<i>priority-number</i>	Select one of the following as the priority number: • 1—1st priority • 2—2nd priority • 3—3rd priority • 4—4th priority

Command Default

The default download characteristics apply to routes and prefixes downloaded from the Route Processor (RP) to the line cards.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use this command to change the priority of how prefixes and routes in the Cisco Express Forwarding table are downloaded from the RP to the line cards.

Default download priorities are set up to improve convergence when topology changes occur in networks of distributed platform, such as the Cisco 7600 series routers and the Cisco Catalyst 6000 series switches.

Prefixes and routes are categorized and downloaded at four different priorities. [Table 1](#) lists the download priority and the associated prefix or route type.

Table 1 *Download Priorities and Associated Prefix or Route Category*

Download Priority	Prefix or Route Type
Priority 1 (P1)	• Default routes • Routes with recursive dependents, typically Interior Gateway Protocol (IGP) prefixes that are the next hop of internal Border Gateway Protocol (iBGP) learned routes
Priority 2 (P2)	• Directly connected routes • Receive routes; that is, the host routes for the interface address of the router
Priority 3 (P3)	• Any route in a VRF table
Priority 4 (P4)	• Any other route

In a typical network, a small number of IGP prefixes have many iBGP prefixes recursing through them. When an IGP topology change occurs, the key to updating the forwarding of the iBGP prefixes is to update the IGP prefix through which they recurse. If these prefixes with recursing dependents are downloaded before other prefixes, convergence will be faster. Therefore, the default priority for routes with recursive dependents is P1.

Prioritizing the download of directly connected prefixes and their associated local interface address allows for faster and more deterministic failure detection when an interface goes down. In addition, traffic is received at the local interface addresses as soon as possible, which allows for faster Layer 3 protocol convergence. The default priority for directly connected and receive routes is set at P2.

VRF routes over global table routes or Internet routes have a default priority of P3, and all other routes are prioritized at P4.

The **cef table download** command allows you to override a default priority so you can customize prefix and route downloads from the RP to the line cards. To display the configured download priority, use the **show cef table download priority** command.

Examples

The following example shows how to change the download priority of the default route from P1 to P2:

```
Router(config)# cef table download default-route priority 2
```

Related Commands

Command	Description
show cef table download priority	Displays the configured download priority of Cisco Express Forwarding routes.

cef table output-chain build

To configure characteristics for Cisco Express Forwarding table output chain building for the forwarding of packets through the network, use the **cef table output-chain build** command in global configuration mode. To disable Cisco Express Forwarding table output chain-building characteristics, use the **no** form of this command. To restore the general Cisco Express Forwarding table output chain-building characteristics to their default values, use either the **default** form of this command.

General Characteristics

cef table output-chain build favor { convergence-speed | memory-utilization }

no cef table output-chain build favor

default cef table output-chain build favor

Individual Overrides

**cef table output-chain build { indirection [non-recursive-prefix] [recursive-prefix] |
inplace-modify [load-sharing] [push-counter] }**

**no cef table output-chain build { indirection [non-recursive-prefix] [recursive-prefix] |
inplace-modify [load-sharing] [push-counter] }**

**default cef table output-chain build { indirection [non-recursive-prefix] [recursive-prefix] |
inplace-modify [load-sharing] [push-counter] }**

Syntax Description

convergence-speed	Configures a faster convergence speed for table output chain building.
memory-utilization	Configures less memory use for table output chain building.
default	Removes any table output chain building characteristic.
indirection	Enables insertion of indirection objects for table output chain building.
non-recursive-prefix	(Optional) Enables insertion of indirection objects for nonrecursive prefixes.
recursive-prefix	(Optional) Enables insertion of indirection objects for recursive prefixes.
inplace-modify	Enables in-place modification of objects in the forwarding chain.
load-sharing	(Optional) Enables in-place modification of load-balancing objects in the forwarding chain.
push-counter	(Optional) Enables in-place modification of packet counters in the output chain.

Command Default

Convergence speed and indirection characteristics are enabled by default for the building of Cisco Express Forwarding table output chains.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
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**General Characteristics**

Use the **cef table output-chain build favor** command to override the Cisco Express Forwarding table default operational behavior used to build output chains for forwarding of network traffic.

The default behavior for output chain building favors convergence, if this behavior is permitted by the platform. (See your platform documentation for information on the convergence of recursive and nonrecursive prefixes.) Depending on your network requirements and resources, you might choose to do one of the following:

- Use the **convergence-speed** keyword to increase convergence speed, which requires additional system resources, especially additional memory.
- Use the **memory-utilization** keyword to decrease memory use, which decreases convergence speed and uses fewer system resources.

The default is platform-specific and usually sufficient. The default falls between the options provided for your use with this command.

For all **cef table output-chain build** commands, the state is enabled, disabled, or use the system defaults. To remove any configuration you must enter the **default** keyword with the command instead of the **no** keyword. To disable an output chain-building characteristic, enter the **no** keyword.

The output of the **show cef table** command displays the current configuration and operational state of the Cisco Express Forwarding table.

Individual Overrides

This command is used for troubleshooting purposes only.

**Note**

Use this command only on the advice of field personnel from Cisco.

The use of the **cef table output-chain build** command with either the **indirection** or **inplace-modify** keyword overrides specific Cisco Express Forwarding table output chain-building behavior. Indirection characteristics are installed by default if the platform supports or permits their use.

The **indirection** keyword enables or disables the insertion of indirection objects for recursive or nonrecursive prefixes or for both recursive and nonrecursive prefixes. Inserting an indirection object into the forwarding chain allows the handling of any aggregate event that affects multiple prefixes by the modification of the indirection object. For example, if a number of recursive prefixes all share the same recursive nexthop, and the route to the recursive nexthop changes, a single update to an indirection object can restore forwarding for those recursive prefixes.

If you configure the **cef table output-chain build indirection** command without a prefix type, recursive and nonrecursive prefixes are explicitly enabled. This command would override any preference configured with the existing **cef table output-chain build favor** command.

The **inplace-modify** keyword enables or disables the ability to modify certain objects in the forwarding chain by modifying the data that an object holds. The alternative is a complete replacement of the object and the relinking of all links to the object.

To return to system default settings for Cisco Express Forwarding table output chain building, use the **default** form of the command.

The output of the **show cef table** command displays the current configuration and operational state of the Cisco Express Forwarding table.

Examples

The following example shows how to configure the use of less memory for table output chain building:

```
Router(config)# cef table output-chain build favor memory
```

Use this command if your priority is to save memory and your network does not require a faster convergence speed for table output chain building for forwarding of network traffic.

Related Commands

Command	Description
show cef table	Displays the configuration and operational state of the FIB.
show ip cef switching statistics	Displays switching statistics in the FIB.
show ipv6 cef switching statistics	Displays switching statistics in the IPv6 FIB.

cef table rate-monitor-period

To set a time period over which to calculate the rate of route updates from the Routing Information Base (RIB) to the Cisco Express Forwarding Forwarding Information Base (FIB) tables, use the **cef table rate-monitor-period** command in global configuration mode. To return to the default time period, use the **no** form of this command.

cef table rate-monitor-period *minutes*

no cef table rate-monitor-period *minutes*

Syntax Description	<i>minutes</i>	The time period, in minutes, over which to calculate the rate of route updates to Cisco Express Forwarding tables. The range is from 1 to 60. The default is 5.
---------------------------	----------------	---

Command Default	If the command is not configured, the sampling rate is every 5 minutes.
------------------------	---

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

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 change the sampling rate period over which to monitor route updates from the RIB to the Cisco Express Forwarding IPv4 and IPv6 FIB tables. Changing the sampling period allows you to calculate the rate of route insertion into the FIB at any interval length from 1 minute to 60 minutes.
-------------------------	--

Examples	The following example shows how to set the time period to 1 minute over which to calculate the rate of route updates from the RIB to the IPv4 FIB and IPv6 FIB:
-----------------	---

```
Router(config)# cef table rate-monitor-period 1
```

Related Commands	Command	Description
	show cef table	Displays the configuration and operational state of the Cisco Express Forwarding FIB table.

clear adjacency

To clear the Cisco Express Forwarding adjacency table, use the **clear adjacency** command in privileged EXEC mode.

clear adjacency

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	11.2GS	This command was introduced to support the Cisco 12012 Internet router.
	11.1CC	Support was added for multiple platforms.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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.
	12.2(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 Using the **clear adjacency** command repopulates adjacencies from sources. Any remaining stale adjacencies (meaning those that fail to repopulate on request) are then purged. Layer 2 next hop information is reevaluated.

Clearing adjacencies cause the adjacency table to repopulate from the Layer 2 to Layer 3 mapping tables. To reevaluate the mappings, clear the source information by using a Cisco IOS command, such as the **clear arp-cache** command.

For Cisco 7500 Routers

On a distributed system, the adjacency tables that reside on line cards are always synchronized to the adjacency table that resides on the Route/Switch Processor (RSP). Refreshing the adjacencies also refreshes adjacencies on line cards and purges stale entries. (Entering the **clear adjacency** command on a line card has no effect.)

Examples The following example clears the adjacency table:

```
Router# clear adjacency
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
debug adjacency	Enables the display of information about the adjacency database.
show adjacency	Displays Cisco Express Forwarding adjacency table information.
show mls cef adjacency	Displays information about the hardware Layer 3 switching adjacency node.

clear adjacency epoch

**Note**

The **clear adjacency epoch** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases.

To begin a new epoch and increment the epoch number of the Cisco Express Forwarding adjacency table, use the **clear adjacency epoch** command in privileged EXEC mode.

clear adjacency epoch

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2S releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Usage Guidelines

The **clear adjacency epoch** command increments the epoch and flushes entries with the old epoch. This command clears inconsistencies.

Use the **clear adjacency epoch** command when you want to rebuild the adjacency table. A new adjacency table might be required because the user wants to remove inconsistencies from the table.

Examples

The following example shows how to begin a new epoch and increments the epoch number of the adjacency table:

```
Router# clear adjacency epoch
```

clear cef interface

To clear the Cisco Express Forwarding per-interface traffic policy statistics for an interface, use the **clear cef interface** command in privileged EXEC mode.

clear cef interface [*interface-type interface-number*] **policy-statistics**

Syntax Description

<i>interface-type</i>	Type of interface to clear the policy statistics for
<i>interface-number</i>	Port, connector, or interface card number
policy-statistics	Policy statistics for the specified interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(9)S	This command was introduced to support the Cisco 12000 series Internet routers.
12.0(17)ST	This command was introduced to support the Cisco 12000 series Internet routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command clears the Cisco Express Forwarding Border Gateway Protocol (BGP) traffic policy statistics counters for an interface.

If you do not specify an interface type and interface number the policy statistics for all interfaces are cleared.

Examples

The following example clears the Cisco Express Forwarding BGP traffic policy statistics counters:

```
Router# clear cef interface ethernet 0/0 policy-statistics
Router#
```

Related Commands

Command	Description
bgp-policy	Enables BGP policy accounting or policy propagation on an interface.
show cef interface policy-statistics	Displays detailed Cisco Express Forwarding policy statistical information for all interfaces.

clear cef linecard

To clear Cisco Express Forwarding information from line cards, use the **clear cef linecard** command in privileged EXEC mode.

clear cef linecard [*slot-number*] [**adjacency** | **interface** | **prefix**]

Syntax Description

<i>slot-number</i>	(Optional) Line card slot number to clear. When you omit this argument, all line card slots are cleared.
adjacency	(Optional) Clears line card adjacency tables and rebuilds adjacency for the specified line card.
interface	(Optional) Clears line card interface information and recreates the interface information for the specified line card.
prefix	(Optional) Clears line card prefix tables and starts rebuilding the Forwarding Information Base (FIB) table.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2GS	This command was introduced to support the Cisco 12012 Internet router.
11.1CC	Support was added for multiple platforms.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 7000 series router. This command is not supported on the Cisco 10000 series router.
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.

Usage Guidelines

This command is available only on distributed platforms (such as the Cisco 7500 series) running distributed Cisco Express Forwarding.

Cisco Express Forwarding information on the line cards is cleared; however, Cisco Express Forwarding information on the Route Processor (RP) is not affected.

After you clear Cisco Express Forwarding information from line cards, the corresponding information from the RSP is propagated to the line cards. Interprocess communications (IPC) ensures that Cisco Express Forwarding information on the Route Switch Processor (RSP) matches the Cisco Express Forwarding information on the line cards.

Because this command might require significant processing resources and can cause dropped traffic or system error messages about excessive CPU use, its use is recommended only as a last resort for debugging or mitigating serious problems.



Note

Cisco 10000 series routers do not support the **clear cef linecard** command.

Examples

The following example clears the Cisco Express Forwarding information from the line cards:

```
clear cef linecard
```

Related Commands

Command	Description
show cef linecard	Displays Cisco Express Forwarding-related interface information by line card.

clear cef table

To clear the Cisco Express Forwarding tables, use the **clear cef table** command in privileged EXEC mode.

```
clear cef table {ipv4 | ipv6} [vrf {vrf-name | * }]
```

Syntax Description

ipv4	Clears the Cisco Express Forwarding tables for IPv4 addresses.
ipv6	Clears the Cisco Express Forwarding tables for IPv6 addresses.
Note	On the Cisco 10000 series routers IPv6 is supported on Cisco IOS Release 12.2(28)SB and later releases.
vrf	(Optional) Specifies all VPN routing and forwarding (VRF) instance tables or a specific VRF table for an IPv4 or IPv6 address.
<i>vrf-name</i>	(Optional) Clears the specific VRF table for IPv4 or IPv6 addresses.
*	(Optional) Clears all the VRF tables for IPv4 or IPv6 addresses.

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

The **clear cef table** command clears the selected table or address family of tables (for IPv4 or IPv6) and updates (refreshes) them throughout the router (including the Route Processor and line cards). The command increments the table epoch, updates the tables, distributes the updated information to the line cards, and performs a distributed purge of any stale entries in the tables based on the noncurrent epoch number. This ensures that any inconsistencies that occurred over time are removed.

Because this command might require significant processing resources and can cause dropped traffic or system error messages about excessive CPU use, its use is recommended only as a last resort for debugging or mitigating serious problems.

Cisco Express Forwarding tables are also cleared automatically during bootup or online insertion and removal (OIR) of line cards.

Note On the Cisco 10000 series routers, IPv6 is supported on Cisco IOS Release 12.2(28)SB or later releases.

Examples

The following example clears the Cisco Express Forwarding tables for the IPv6 address family:

```
Router# clear cef table ipv6 vrf *
```

The following example clears the Cisco Express Forwarding tables for a VRF table named vrf1 in the IPv4 address family:

```
Router# clear cef table ipv4 vrf vrf1
```

The following example clears the Cisco Express Forwarding tables for all VRF tables in the IPv4 address family. This example shows output with Cisco Express Forwarding table debugging enabled:

```
Router# clear cef table ipv4 vrf *
```

```
06:56:01: FIBtable: Refreshing table IPv4:Default
06:56:01: FIBtable: Invalidated 224.0.0.0/4 in IPv4:Default
06:56:01: FIBtable: Deleted 224.0.0.0/4 from IPv4:Default
06:56:01: FIBtable: Validated 224.0.0.0/4 in IPv4:Default
06:56:01: FIBtable: IPv4: Event up, 10.1.41.0/24, vrf Default, 1 path, flags 0100
0220
06:56:01: FIBtable: IPv4: Adding route for 10.1.41.0/24 but route already exists.
Trying modify.
06:56:01: FIBtable: IPv4: Event up, 10.0.0.11/32, vrf Default, 1 path, flags 010
00000
06:56:01: FIBtable: IPv4: Adding route for 10.0.0.11/32 but route already exists
. Trying modify.
06:56:01: FIBtable: IPv4: Event up, 10.0.0.15/32, vrf Default, 1 path, flags 010
00000
06:56:01: FIBtable: IPv4: Adding route for 10.0.0.15/32 but route already exists
. Trying modify.
06:56:01: FIBtable: IPv4: Event up, 10.0.0.7/32, vrf Default, 1 path, flags 0100
0220
06:56:01: FIBtable: IPv4: Adding route for 10.0.0.7/32 but route already exists.
Trying modify.
06:56:01: FIBtable: IPv4: Event up, 10.0.0.0/8, vrf Default, 1 path, flags 00000
220
06:56:01: FIBtable: IPv4: Adding route for 10.0.0.0/8 but route already exists.
Trying modify.
06:56:01: FIBtable: IPv4: Event up, 0.0.0.0/0, vrf Default, 1 path, flags 004200
05
06:56:01: FIBtable: IPv4: Adding route for 0.0.0.0/0 but route already exists. T
rying modify.
06:56:01: FIBtable: Starting purge of table IPv4:Default to epoch 13
06:56:01: FIBtable: Invalidated 10.1.41.1/32 in IPv4:Default
06:56:01: FIBtable: Deleted 10.1.41.1/32 from IPv4:Default
06:56:01: FIBtable: Purged 1 prefix from table IPv4:Default
06:56:01: FIBtable: Validated 10.1.41.1/32 in IPv4:Default
06:56:06: FIBtable: IPv4: Event modified, 0.0.0.0/0, vrf Default, 1 path, flags
00420005
06:56:06: FIBtable: IPv4: Event up, default, 0.0.0.0/0, vrf Default, 1 path, fla
gs 00420005
06:56:06: FIBtable: IPv4: Adding route for 0.0.0.0/0 but route already exists. T
rying modify.
```

Related Commands	Command	Description
	clear ip cef inconsistency	Clears Cisco Express Forwarding inconsistency statistics and records found by the Cisco Express Forwarding consistency checkers.
	debug cef	Enables the display of information about Cisco Express Forwarding events.
	debug ip cef table	Enables the collection of events that affect entries in the Cisco Express Forwarding tables.
	show cef table consistency-check	Displays Cisco Express Forwarding consistency checker table values.
	show ip cef inconsistency	Displays Cisco Express Forwarding IP prefix inconsistencies.

clear ip cache

To delete entries in the routing table cache used to fast switch IP traffic, use the **clear ip cache** command in privileged EXEC mode.

clear ip cache [*prefix mask*]

Syntax Description

<i>prefix mask</i>	(Optional) Deletes only the entries in the cache that match the prefix and mask combination.
--------------------	--

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to clear routes from the routing table cache. You can remove all entries in the routing cache or you can remove only those entries associated with a specified prefix and mask.



Note

IPv4 fast switching is not supported in Cisco IOS 12.4(20)T and later releases.

Examples

The following command shows how to delete the all of the entries in the routing table cache:

```
Router# clear ip cache
```

The following command show how to delete entries in the router table associated with the prefix and mask 192.168.32.0 255.255.255.0:

```
Router# clear ip cache 192.168.32.0 255.255.255.0
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
show ip cache	Displays the routing table cache used to fast switch IP traffic.

clear ip cef epoch



Note

The **clear ip cef epoch** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases.

To begin a new epoch and increment the epoch number for one or all Cisco Express Forwarding tables, use the **clear ip cef epoch** command in privileged EXEC mode.

clear ip cef epoch [**all-vrfs** | **full** | **vrf** *[table]*]

Syntax Description

all-vrfs	(Optional) Begins a new epoch for all Forwarding Information Base (FIB) tables.
full	(Optional) Begins a new epoch for all tables, including adjacency tables.
vrf	(Optional) Begins a new epoch for the specified FIB table.
<i>table</i>	(Optional) Virtual Private Network (VPN) routing and forwarding (VRF) instance name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2SX releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Usage Guidelines

Use the **clear ip cef epoch** command when you want to rebuild a table. This command increments the epoch number and flushes entries with the old epoch number. This command clears any inconsistencies that might exist, so if everything in the system is working correctly, this command does not affect the Cisco Express Forwarding forwarding tables other than changing the current epoch values.

Examples

The following example shows the output before and after you clear the epoch table and increment the epoch number:

```
Router# show ip cef epoch
```

```
CEF epoch information:
```

```
Table: Default-table
```

```
Table epoch: 2 (43 entries at this epoch)
```

```
Adjacency table
```

```
Table epoch: 2 (5 entries at this epoch)
```

```
Router# clear ip cef epoch full
```

```
Router# show ip cef epoch
```

```
CEF epoch information:
```

```
Table: Default-table
```

```
Table epoch: 3 (43 entries at this epoch)
```

```
Adjacency table
```

```
Table epoch: 3 (5 entries at this epoch)
```

Related Commands

Command	Description
show cef state	Displays the state of Cisco Express Forwarding.
show ip cef epoch	Displays the table epochs of the adjacency table and of all FIB tables.

clear ip cef epoch full

To begin a new epoch and increment the epoch number for all Cisco Express Forwarding tables (including the adjacency table), use the **clear ip cef epoch full** command in privileged EXEC mode.

clear ip cef epoch full

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2(14)SX	This command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines Use the **clear ip cef epoch full** command when you want to rebuild a table. This command allows old and new table entries to be distinguished within the same data structure and allows you to retain the old Cisco Express Forwarding database table while constructing the new table.

These **show** commands display epoch information:

- **show ip cef summary**—Displays the table epoch for a specific Forwarding Information Base (FIB) table.
- **show ip cef detail**—Displays the epoch value for each entry of a specific FIB table.
- **show adjacency summary**—Displays the adjacency table epoch.
- **show adjacency detail**—Displays the epoch value for each entry of the adjacency table.

Examples This example shows the output before and after you clear the epoch table and increment the epoch number:

```
Router# show ip cef epoch

CEF epoch information:

Table:Default-table
  Table epoch:2 (164 entries at this epoch)

Adjacency table
  Table epoch:1 (33 entries at this epoch)
```

clear ip cef epoch full

```
Router# clear ip cef epoch full
Router# show ip cef epoch

CEF epoch information:

Table:Default-table
  Table epoch:3 (164 entries at this epoch)

Adjacency table
  Table epoch:2 (33 entries at this epoch)
```

Related Commands

Command	Description
show adjacency detail	Displays the information about the protocol detail and timer.
show adjacency summary	Displays a summary of Cisco Express Forwarding adjacency information.
show ip cef detail	Displays detailed FIB entry information.
show ip cef summary	Displays a summary of the FIB.

clear ip cef event-log

**Note**

Effective with Cisco IOS 12.2(25)S, the **clear ip cef event-log** command is replaced by the **monitor event-trace cef ipv4 clear** command. See the **monitor event-trace** (EXEC) command for more information.

To clear the Cisco Express Forwarding event-log buffer, use the **clear ip cef event-log** command in privileged EXEC mode.

clear ip cef event-log

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(25)S	This command was replaced by the monitor event-trace cef ipv4 clear command.
12.2(33)SRA	This command was replaced by the monitor event-trace cef ipv4 clear command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was replaced by the monitor event-trace cef ipv4 clear command.

Usage Guidelines

This command clears the entire Cisco Express Forwarding table event log that holds Forwarding Information Base (FIB) and adjacency events.

Examples

The following example shows how to clear the Cisco Express Forwarding event-log buffer:

```
Router# clear ip cef event-log
```

 clear ip cef event-log**Related Commands**

Command	Description
cef table consistency-check	Enables Cisco Express Forwarding table consistency checker types and parameters.
ip cef table event-log	Controls Cisco Express Forwarding table event-log characteristics.
show ip cef events	Displays all recorded Cisco Express Forwarding FIB and adjacency events.

clear ip cef inconsistency

To clear the Cisco Express Forwarding inconsistency checker statistics and records found by the Cisco Express Forwarding consistency checkers, use the **clear ip cef inconsistency** command in privileged EXEC mode.

clear ip cef inconsistency

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.0(15)S	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	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(17d)SXB release.
	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)SR.
	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 This command clears the Cisco Express Forwarding inconsistency checker statistics and records that accumulate when the **cef table consistency-check** command is enabled.

Examples The following example shows how to clear all Cisco Express Forwarding inconsistency checker statistics and records:

```
Router# clear ip cef inconsistency
```

 **clear ip cef inconsistency**

Related Commands	Command	Description
	cef table consistency-check	Enables Cisco Express Forwarding table consistency checker types and parameters.
	show ip cef inconsistency	Displays Cisco Express Forwarding IP prefix inconsistencies.

clear ip cef prefix-statistics

To clear Cisco Express Forwarding counters by resetting the packet and byte count to zero (0), use the **clear ip cef prefix-statistics** command in privileged EXEC mode.

clear ip cef *network* [*mask*] **prefix-statistics**

Syntax Description

<i>network</i>	Forwarding Information Base (FIB) entry specified by network.
<i>mask</i>	(Optional) FIB entry specified by network and mask.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2GS	This command was introduced to support the Cisco 12012 Internet router.
11.1CC	Support for multiple platform was added.
12.2(25)S	The * (asterisk) keyword was removed.
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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

When the clear statistics flag is set, statistics are cleared as the FIB table is scanned. The time period is up to 60 seconds for all statistics to clear. However, clearing a specific prefix is completed immediately.

Examples

The following example shows how to reset the packet and byte counts to zero for Cisco Express Forwarding entries on the 172.17.10.10 network:

```
Router# clear ip cef 172.17.10.10 prefix-statistics
```

Related Commands

Command	Description
ip cef accounting	Enables Cisco Express Forwarding network accounting.
show adjacency	Displays Cisco Express Forwarding adjacency table information.
show ip cef	Displays entries or a summary of the FIB table.

clear ip mds

To clear multicast distributed switching (MDS) information from the router, use the **clear ip mds** command in privileged EXEC mode.

clear ip mds { **all** | [**vrf** *vrf-name*] **forwarding** }

Syntax Description

all	Clear all IP MDS information.
vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
forwarding	Clears all linecard routes from a Multicast Forwarding Information Base (MFIB) table and resynchronizes it with the Route Processor (RP).

Command Modes

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

Cisco 12000 Series Internet Router

On a Cisco 12000 series Internet router the **clear ip mds** command must be run in privileged EXEC mode on a linecard.

Examples

The following example clears all line card routes in an MFIB table on a Cisco 12000 series Internet router:

```
Router# attach 1
LC-Slot1> enable
LC-Slot1# clear ip mds forwarding
```

The following example clears all line card routes in an MFIB table on a Cisco 7500 series router:

```
Router# clear ip mds forwarding
```


Related Commands

Command	Description
show ip mds interface	Displays the MFIB table and forwarding information for MDS on a line card.
show ip mds stats	Display switching statistics or line card statistics for MDS.
show ip mds summary	Displays a summary of the MFIB table for MDS.
show ip mds forwarding	Displays MDS information for all the interfaces on the line card.

clear ip mds forwarding

The **forwarding** keyword for the **clear ip mds** command is no longer documented as a separate command.

The information for using the **forwarding** keyword for the **clear ip mds** command has been incorporated into the **clear ip mds** command documentation. See the **clear ip mds** command documentation for more information.

clear ip mds linecard

To reset multicast distributed switching (MDS) line card information on the router, use the **clear ip mds linecard** command in privileged EXEC mode.

```
clear ip mds linecard {linecard-slot-number | *}
```

Syntax Description

<i>linecard-slot-number</i>	Slot number containing the line card to be reset.
*	Indicates that the reset should be executed on all line cards.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(19.3)S	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

When the * keyword is specified instead of the *linecard-slot-number* argument, all MDS information on all line cards is cleared and reset.

Examples

The following example clears and resets all MDS line card information on the router:

```
Router# clear ip mds linecard *
```

Related Commands

Command	Description
show ip mds	Clears MDS information from the router.
show ip mds interface	Displays the MFIB table and forwarding information for MDS on a line card.
show ip mds stats	Display switching statistics or line card statistics for MDS.
show ip mds summary	Displays a summary of the MFIB table for MDS.
show ip mds forwarding	Displays MDS information for all the interfaces on the line card.

clear ip traffic

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

clear ip traffic [*interface type number*]

Syntax Description

interface type number (Optional) Clears 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 **clear ip traffic** command with no keywords or arguments clears the global or system-wide IP traffic statistics for all interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.1S	This command was modified to include the optional interface keyword and associated <i>type</i> and <i>number</i> arguments. These modifications were made to provide support for the IPv4 MIBs as described in RFC 4293, <i>Management Information Base for the Internet Protocol (IP)</i> .

Usage Guidelines

Using the **clear ip traffic** command with the optional **interface** keyword clears the `ipIfStatsTable` counters displayed for the specified interface and also clears the counters displayed by the **show ip traffic interface** command.

Examples

The following example clears the global or system-wide IP traffic statistics on all interfaces:

```
Router# clear ip traffic
```

Related Commands

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

clear mls cef ip accounting per-prefix

To clear information about the IP per-prefix accounting statistics, use the **clear mls cef ip accounting per-prefix** command in privileged EXEC mode.

clear mls cef ip accounting per-prefix {all | {*prefix mask* [*instance*]}}

Syntax Description

all	Clears all per-prefix accounting statistics information.
<i>prefix</i>	Entry prefix in the format A.B.C.D.
<i>mask</i>	Entry prefix mask.
<i>instance</i>	(Optional) VPN routing and forwarding instance name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17a)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.

Examples

This example shows how to clear all information about the per-prefix accounting statistics:

```
Router# clear mls cef ip accounting per-prefix all
```

clear pxf

To clear Parallel eXpress Forwarding (PXF) counters and statistics, use the **clear pxf** command in privileged EXEC mode.

```
clear pxf [dma counters | interface interface | statistics {context | diversion | drop | ip | ipv6} | xcm counters]
```

Syntax Description

dma counters	(Optional) Clears the direct memory access (DMA) PXF counters.
interface <i>interface</i>	(Optional) Clears the PXF counters on the specified interface.
statistics	(Optional) Type of PXF statistics to clear. The options are: • context—Current and historical loads on the PXF. • diversion—Traffic diverted from the PXF. • drop—Dropped packets and bytes. • ip—IP and ICMP statistics. • ipv6—IPv6 statistics.
xcm counters	Clears the PXF Error Code Correction (ECC) counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced on the Cisco 10000 series router.
12.2(1)XF1	This command was introduced on the Cisco uBR10012 router.
12.2(4)XF1	The xcm counters option was introduced to support the Performance Routing Engine (PRE1) module on the Cisco uBR10012 router.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC. The context and ipv6 keyword options are not supported.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. The ipv6 keyword option is not supported.

Usage Guidelines

If no interface is specified, the command clears PXF counters on all interfaces. The **clear pxf** command clears counters associated with the **show pxf dma**, **show pxf interface**, **show pxf statistics**, and **show pxf xcm** commands.

Cisco uBR10012 Universal Broadband Router

Not all keyword options are supported in the Cisco IOS software for the Cisco uBR10012 universal broadband router. See the command history table for the unsupported keyword options by release.

The **clear pxf xcm counters** command is supported only on the PRE1 and later processors for the Cisco uBR10012 router. This command is not supported on the PRE processor.

Examples

The following example clears PXF statistics for serial interface 1/0/0:

```
Router# clear pxf interface serial 1/0/0
```

The following example clears PXF statistics on all interfaces:

```
Router# clear pxf interface
```

Related Commands

Command	Description
show pxf cpu statistics	Displays PXF CPU statistics.
show pxf dma	Displays the current state of DMA buffers, error counters, and registers on the PXF engine.
show pxf interface	Displays a summary of the statistics accumulated by column 0 of the PXF for an interface.
show pxf statistics	Displays chassis-wide, summary PXF statistics.
show pxf xcm	Displays PXF XCM information.

ip cache-invalidate-delay

To control the invalidation rate of the IP route cache, use the **ip cache-invalidate-delay** command in global configuration mode. To allow the IP route cache to be immediately invalidated, use the **no** form of this command.

ip cache-invalidate-delay [*minimum maximum quiet threshold*]

no ip cache-invalidate-delay

Syntax Description

<i>minimum</i>	(Optional) Minimum time (in seconds) between invalidation request and actual invalidation. The default is 2 seconds.
<i>maximum</i>	(Optional) Maximum time (in seconds) between invalidation request and actual invalidation. The default is 5 seconds.
<i>quiet</i>	(Optional) Length of quiet period (in seconds) before invalidation. The default is 3 seconds with no more than zero invalidation requests.
<i>threshold</i>	(Optional) Maximum number of invalidation requests considered to be quiet.

Command Default

The invalidation rate of the IP route cache is not controlled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	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

After you enter the **ip cache-invalidate-delay** command all cache invalidation requests are honored immediately.



Caution

This command should only be used under the guidance of technical support personnel. Incorrect settings can seriously degrade network performance. The command-line-interface (CLI) will not allow you to enter the **ip cache-invalidate-delay** command until you configure the **service internal** command in global configuration mode.

The IP fast-switching and autonomous-switching features maintain a cache of IP routes for rapid access. When a packet is to be forwarded and the corresponding route is not present in the cache, the packet is process switched and a new cache entry is built. However, when routing table changes occur (such as when a link or an interface goes down), the route cache must be flushed so that it can be rebuilt with up-to-date routing information.

This command controls how the route cache is flushed. The intent is to delay invalidation of the cache until after routing has settled down. Because route table changes tend to be clustered in a short period of time, and the cache may be flushed repeatedly, a high CPU load might be placed on the router.

When this feature is enabled, and the system requests that the route cache be flushed, the request is held for at least *minimum* seconds. Then the system determines whether the cache has been “quiet” (that is, less than *threshold* invalidation requests in the last *quiet* seconds). If the cache has been quiet, the cache is then flushed. If the cache does not become quiet within *maximum* seconds after the first request, it is flushed unconditionally.

Manipulation of these parameters trades off CPU utilization versus route convergence time. Timing of the routing protocols is not affected, but removal of stale cache entries is affected.

Examples

The following example shows how to set a minimum delay of 5 seconds, a maximum delay of 30 seconds, and a quiet threshold of no more than 5 invalidation requests in the previous 10 seconds:

```
Router(config)# service internal
Router(config)# ip cache-invalidate-delay 5 30 10 5
```

Related Commands

Command	Description
ip route-cache	Configures the high-speed switching caches for IP routing.

ip cef

To enable Cisco Express Forwarding on the route processor card, use the **ip cef** command in global configuration mode. To disable Cisco Express Forwarding, use the **no** form of this command.

Cisco IAD2420 Series Routers, Cisco 2600 Series Routers, Cisco 3600 Series Routers, Cisco 3700 Series Routers, Cisco 7200 Series Routers

ip cef [distributed]

no ip cef [distributed]

Cisco ASR 1000 Series Aggregation Services Routers

ip cef distributed

no ip cef distributed

Syntax Description

distributed	(Optional) Enables distributed Cisco Express Forwarding operation. Distributes Cisco Express Forwarding information to line cards. Line cards perform express forwarding.
--------------------	---

Command Default

Cisco Express Forwarding is enabled by default on most platforms. To find out if Cisco Express Forwarding is enabled by default on your platform, enter the **show ip cef** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2	The default for Cisco 7200 series routers was changed from disabled to enabled.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the following platforms: Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640 routers, Cisco 3660 routers, Cisco 3700 series routers, and Cisco MC3810 multiservice access concentrators.
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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **ip cef** command is not available on the Cisco 12000 series because that router series operates only in distributed Cisco Express Forwarding mode. Distributed Cisco Express Forwarding is enabled also on the Cisco 6500 series router.

Cisco Express Forwarding is advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

If you enable Cisco Express Forwarding and then create an access list that uses the **log** keyword, the packets that match the access list are not Cisco Express Forwarding switched. They are fast switched. Logging disables Cisco Express Forwarding.

The following example shows how to enable standard Cisco Express Forwarding operation:

```
Router(config)# ip cef
```

The following example shows how to enable distributed Cisco Express Forwarding operation:

```
Router(config)# ip cef distributed
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
ip cef accounting	Enables Cisco Express Forwarding network accounting.
ip cef load-sharing algorithm	Selects a Cisco Express Forwarding load balancing algorithm.
ip cef table adjacency-prefix override	Enables Cisco Express Forwarding adjacency prefixes to override static host glean routes.
cef table consistency-check	Enables Cisco Express Forwarding table consistency checker types and parameters.
show ip cef	Displays entries or a summary of the FIB table.

ip cef accounting

To enable Cisco Express Forwarding network accounting, use the **ip cef accounting** command in global configuration mode or interface configuration mode. To disable network accounting of Cisco Express Forwarding, use the **no** form of this command.

ip cef accounting *accounting-types*

no ip cef accounting *accounting-types*

Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode

ip cef accounting non-recursive { **external** | **internal** }

no ip cef accounting non-recursive { **external** | **internal** }

Syntax Description		
	<i>accounting-types</i>	The <i>accounting-types</i> argument must be replaced with at least one of the following keywords. Optionally, you can follow this keyword by any or all of the other keywords, but you can use each keyword only once. • load-balance-hash—Enables load balancing hash bucket counters. • non-recursive—Enables accounting through nonrecursive prefixes. • per-prefix—Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix). • prefix-length—Enables accounting through prefix length.
	non-recursive	Enables accounting through nonrecursive prefixes. This keyword is optional when used in global configuration mode after another keyword is entered. See the <i>accounting-types</i> argument.
	external	Counts input traffic in the nonrecursive external bin.
	internal	Counts input traffic in the nonrecursive internal bin.

Command Default Accounting is disabled by default.

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

Command History	Release	Modification
	11.2GS	This command was introduced.
	11.1CC	Multiple platform support was added and the prefix-length keyword was added.

Release	Modification
12.2(2)T	The ip cef accounting non-recursive command in interface configuration mode was added.
12.2(25)S	The load-balance-hash keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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

Collecting statistics can help you better understand Cisco Express Forwarding patterns in your network.

When you enable network accounting for Cisco Express Forwarding from global configuration mode, accounting information is collected at the Route Processor (RP) when Cisco Express Forwarding mode is enabled and at the line cards when distributed Cisco Express Forwarding mode is enabled. You can then display the collected accounting information using the **show ip cef** privileged EXEC command.

For prefixes with directly connected next hops, the **non-recursive** keyword enables express forwarding of the collection of packets and bytes through a prefix. This keyword is optional when this command is used in global configuration mode.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the **show ip cef detail** command.

Per-destination load balancing uses a series of 16 hash buckets into which the set of available paths are distributed. A hash function operating on certain properties of the packet is applied to select a bucket that contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the **load-balance-hash** keyword with the **ip cef accounting** command to enable per-hash-bucket counters. Enter the **show ip cef prefix internal** command to display the per-hash-bucket counters.

Examples

The following example shows how to enable the collection of Cisco Express Forwarding accounting information for prefixes directly connected to the next hops:

```
Router(config)# ip cef accounting non-recursive
```

Related Commands

Command	Description
ipv6 cef accounting	Enables Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) network accounting.
show cef	Displays information about packets forwarded by Cisco Express Forwarding.
show ip cef	Displays entries or a summary of the FIB table.

ip cef linecard ipc memory

To configure the line card memory pool for the Cisco Express Forwarding queuing messages, use the **ip cef linecard ipc memory** command in global configuration mode. To return to the default Inter-process Communications (IPC) memory allocation, use the **no** form of this command.

ip cef linecard ipc memory *kbps*

no ip cef linecard ipc memory *kbps*

Syntax Description	<i>kbps</i>	Kilobytes of line card memory allocated. Range is 0 to 12800. The default IPC memory allocation is 25 messages. However, this value depends on the switching platform.
---------------------------	-------------	--

Command Default	If you do not configure a line card memory pool for the Cisco Express Forwarding queuing messages, the default is the IPC memory allocation for the switching platform.
------------------------	---

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

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Usage Guidelines	This command is available only on distributed switching platforms.
	If you are expecting large routing updates to the Route Processor (RP), use this command to allocate a larger memory pool on the line cards for queuing Cisco Express Forwarding routing update messages. The memory pool reduces the transient memory requirements on the RP.
	To display and monitor the current size of the Cisco Express Forwarding message queues, use the show cef linecard command. Also, the peak size is recorded and displayed when you use the detail keyword.

Examples	The following example shows how to configure the Cisco Express Forwarding line card memory queue to 128000 kilobytes per second:
-----------------	--

```
Router(config)# ip cef linecard ipc memory 128000
```

Related Commands	Command	Description
	show cef linecard	Displays detailed Cisco Express Forwarding information for the specified line card.

ip cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm, use the **ip cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

```
ip cef load-sharing algorithm { original | tunnel [id] | universal [id] | include-ports { source [id]
| [destination] [id] | source [id] destination [id]} }
```

```
no ip cef load-sharing algorithm
```

Syntax Description		
original		Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.
tunnel		Sets the load-balancing algorithm for use in tunnel environments or in environments where there are only a few IP source and destination address pairs.
<i>id</i>		(Optional) Fixed identifier.
universal		Sets the load-balancing algorithm to the universal algorithm that uses a source and destination and an ID hash.
include-ports source		Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 source port.
include-ports destination		Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 destination port.
include-ports source destination		Sets the load balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.

Command Default	The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.
------------------------	--

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

Command History	Release	Modification
	12.0(12)S	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(11)T	The include-ports source , include-ports destination , and the include-ports source destination keywords were added for the command.
	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

The original Cisco Express Forwarding load-balancing algorithm produced distortions in load sharing across multiple routers because of the use of the same algorithm on every router. When the load-balancing algorithm is set to universal mode, each router on the network can make a different load sharing decision for each source-destination address pair, and that resolves load-balancing distortions.

The tunnel algorithm is designed to share the load more fairly when only a few source-destination pairs are involved.

The include-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not loadshared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams. The include-ports algorithm is available in Cisco IOS Release 12.4(11)T and later releases.

Examples

The following example shows how to enable the Cisco Express Forwarding load-balancing algorithm for tunnel environments:

```
configure terminal
!  
ip cef load-sharing algorithm tunnel  
exit
```

Related Commands

Command	Description
debug ip cef hash	Records Cisco Express Forwarding load-balancing hash algorithm events
ip load-sharing	Enables load balancing for Cisco Express Forwarding.

ip cef optimize neighbor resolution

To configure address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors, use the **ip cef optimize neighbor resolution** command in global configuration mode. To disable address resolution optimization from Cisco Express Forwarding for directly connected neighbors, use the **no** form of this command.

ip cef optimize neighbor resolution

no ip cef optimize neighbor resolution

Syntax Description This command has no arguments or keywords.

Command Default If this command is not configured, Cisco Express Forwarding does not optimize the address resolution of directly connected neighbors for IPv4.

Command Modes Global configuration (config)

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 The **ip cef optimize neighbor resolution** command is very similar to the **ipv6 cef optimize neighbor resolution** command, except that it is IPv4-specific.

Use this command to trigger Layer 2 address resolution of neighbors directly from Cisco Express Forwarding for IPv4.

Examples The following example shows how to optimize address resolution from Cisco Express Forwarding for directly connected neighbors:

```
Router(config)# ip cef optimize neighbor resolution
```

Related Commands	Command	Description
	ipv6 cef optimize neighbor resolution	Configures address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors.

ip cef table adjacency-prefix

To modify how Cisco Express Forwarding adjacency prefixes are managed, use the **ip cef table adjacency-prefix** command in global configuration mode. To disable Cisco Express Forwarding adjacency prefix management, use the **no** form of this command.

ip cef table adjacency-prefix [**override** | **validate**]

no ip cef table adjacency-prefix [**override** | **validate**]

Syntax Description	override	(Optional) Enables Cisco Express Forwarding adjacency prefixes to override static host glean routes.
	validate	(Optional) Enables the periodic validation of Cisco Express Forwarding adjacency prefixes.

Defaults All Cisco Express Forwarding adjacency prefix management is disabled by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.0(16)S	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.1(13)E07	The validate keyword was added.
	12.1(19.02)E	The default behavior for ip cef table adjacency-prefix override was changed to disabled.
	12.3(04)XG	
	12.3(04)XK	
	12.3(06.01)PI03	
	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 When Cisco Express Forwarding is configured, the forwarding information base (FIB) table may conflict with static host routes that are specified in terms of an output interface or created by a Layer 2 address resolution protocols such as Address Resolution Protocol (ARP), map lists, and so on.

The Layer 2 address resolution protocol adds adjacencies to Cisco Express Forwarding, which in turn creates a corresponding host route entry in the FIB table. This entry is called an adjacency prefix.

override

If the Cisco Express Forwarding adjacency prefix entries are also configured by a static host route, a conflict occurs.

This command ensures that adjacency prefixes can override static host glean routes, and correctly restore routes when the adjacency prefix is deleted.

validate

When you add a /31 netmask route, the new netmask does not overwrite an existing /32 Cisco Express Forwarding entry. This problem is resolved by configuring the **validate** keyword to periodically validate prefixes derived from adjacencies in the FIB against prefixes originating from the RIB.

Examples

override

The following example shows how to enable Cisco Express Forwarding table adjacency prefix override:

```
Router(config)# ip cef table adjacency-prefix override
```

validate

The following example shows how to enable Cisco Express Forwarding table adjacency prefix validation:

```
Router(config)# ip cef table adjacency-prefix validate
```

ip cef table adjacency-prefix

The **override** keyword for the **ip cef table adjacency-prefix** command is no longer documented as a separate command.

The information for using the **override** keyword for the **ip cef table adjacency-prefix** command has been incorporated into the **ip cef table adjacency-prefix** command documentation. See the **ip cef table adjacency-prefix** command documentation for more information.

ip cef table consistency-check



Note

Effective with Cisco IOS Release 12.4(20)T, the **ip cef table consistency-check** command is not available in Cisco IOS software.

To enable consistency checker types and parameters for Cisco Express Forwarding tables, use the **ip cef table consistency-check** command in global configuration mode. To disable consistency checkers, use the **no** form of this command.

```
ip cef table consistency-check [type {lc-detect | scan-lc | scan-rib | scan-rp}] [count
count-number] [period seconds]
```

```
no ip cef table consistency-check [type {lc-detect | scan-lc | scan-rib | scan-rp}] [count
count-number] [period seconds]
```

Suppressing Errors During Route Updates

```
ip cef table consistency-check [settle-time seconds]
```

```
no ip cef table consistency-check [settle-time seconds]
```

Syntax Description

type	(Optional) Specifies the type of consistency check to configure.
lc-detect	(Optional) Specifies that the line card or the module detects a missing prefix. On the line card, a missing prefix is confirmed by Route Processor (RP).
scan-lc	(Optional) Specifies a passive scan check of tables on the line card or module.
scan-rib	(Optional) Specifies a passive scan check of tables on the RP against the Routing Information Base (RIB). For the Cisco 7600 series router, the scan-rib keyword specifies a passive scan check of tables on the rendezvous point against the RIB.
scan-rp	(Optional) Specifies a passive scan check of tables on the RP or on the rendezvous point for the Cisco 7600 series router.
count <i>count-number</i>	(Optional) Specifies the maximum number of prefixes to check per scan. Valid values are from 1 to 225.
period <i>seconds</i>	(Optional) Specifies the period of time between scans. Valid values are from 30 to 3600 seconds.
settle-time <i>seconds</i>	(Optional) Specifies the amount of time that elapsed during which updates for a candidate prefix are ignored as inconsistencies. Valid values are from 1 to 3600 seconds. This keyword is used during route updates.

Command Default

All consistency checkers are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Release 12.2(17d)SXB.
12.2(25)S	This command was replaced by the cef table consistency-check command.
12.2(28)SB	This command was replaced by the cef table consistency-check command.
12.2(33)SRA	This command was replaced by the cef table consistency-check command.
12.2(33)SXH	This command was replaced by the cef table consistency-check command.
12.4(20)T	This command was removed.

Usage Guidelines

This command configures Cisco Express Forwarding table consistency checkers and parameters for the detection mechanism types that are listed in [Table 2](#).

Table 2 CEF Detection Mechanism Types

Detection Mechanism	Where Operates	Description
lc-detect	Line Card or Module	Operates on the line card or module detecting and retrieving IP prefixes that are missing from its FIB table. If IP prefixes are missing, the line card or module cannot forward packets for these addresses. The lc-detect mechanism sends IP prefixes to the RP or rendezvous point for confirmation. If the RP or rendezvous point detects that it has the relevant entry, an inconsistency is identified and an error message is displayed. Also, the RP or rendezvous point sends a signal back to the line card or module confirming that the IP prefix is an inconsistency.
scan-lc	Line Card or Module	Operates on the line card or module by looking through the FIB table for a configurable time period and sending the next <i>n</i> prefixes to the RP or rendezvous point. The RP or rendezvous point performs an exact lookup. If it finds the prefix missing, the RP or rendezvous point reports an inconsistency. Finally, the RP or rendezvous point sends a signal back to the line card or module for confirmation.

Table 2 **CEF Detection Mechanism Types (continued)**

Detection Mechanism	Where Operates	Description
scan-rp	Route Processor	Operates on the RP or rendezvous point (opposite of the scan-lc) by looking through the FIB table for a configurable time period and sending the next <i>n</i> prefixes to the line card or module. The line card or module performs an exact lookup. If it finds the prefix missing, the line card or module reports an inconsistency and finally signals the RP or rendezvous point for confirmation.
scan-rib	Route Processor	Operates on all RPs or rendezvous points (even nondistributed) and scans the RIB to ensure that prefix entries are present in the RP or rendezvous point FIB table.

Examples

The following example shows how to enable the Cisco Express Forwarding consistency checkers:

```
Router(config)# ip cef table consistency-check
```

Related Commands,

Command	Description
clear ip cef inconsistency	Clears Cisco Express Forwarding inconsistency statistics and records found by the Cisco Express Forwarding consistency checkers.
debug ip cef	Displays various Cisco Express Forwarding table query and check events.
show ip cef inconsistency	Displays Cisco Express Forwarding IP prefix inconsistencies.

ip cef table event-log



Note

The **ip cef table event-log** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases.

To control Cisco Express Forwarding table event-log characteristics, use the **ip cef table event-log** command in global configuration mode.

ip cef table event-log [*size event-number*] [**match** *ip-prefix mask*]

no ip cef table event-log [*size event-number*] [**match** *ip-prefix mask*]

Specific to Virtual Private Network (VPN) Event Log

ip cef table event-log [*size event-number*] [**vrf** *vrf-name*] [**match** *ip-prefix mask*]

no ip cef table event-log [*size event-number*] [**vrf** *vrf-name*] [**match** *ip-prefix mask*]

Syntax Description

size <i>event-number</i>	(Optional) Number of event entries. The range is from 1 to 4294967295. The default is 10000.
match	(Optional) Log events matching specified prefix and mask.
<i>ip-prefix</i>	(Optional) IP prefixes matched, in dotted decimal format (A.B.C.D).
<i>mask</i>	(Optional) Network mask written as A.B.C.D.
vrf <i>vrf-name</i>	(Optional) Virtual Private Network (VPN) routing and forwarding instance (VRF) Cisco Express Forwarding table and VRF name.

Defaults

Default size for event log is 10000 entries.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.

Release	Modification
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2SX releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Usage Guidelines

This command is used to troubleshoot inconsistencies that occur in the Cisco Express Forwarding event log between the routes in the Routing Information Base (RIB), Route Processor (RP) Cisco Express Forwarding tables, and line card Cisco Express Forwarding tables.

The Cisco Express Forwarding event log collects Cisco Express Forwarding events as they occur without debugging enabled. This process allows the tracing of an event immediately after it occurs. Cisco technical personnel may ask for information from this event log to aid in resolving problems with the Cisco Express Forwarding feature.

When the Cisco Express Forwarding table event log has reached its capacity, the oldest event is written over by the newest event until the event log size is reset using this command or cleared using the **clear ip cef event-log** command.

Examples

The following example shows how to set the Cisco Express Forwarding table event log size to 5000 entries:

```
Router(config)# ip cef table event-log size 5000
```

Related Commands

Command	Description
cef table consistency-check	Enables Cisco Express Forwarding table consistency checker types and parameters.

ip cef table resolution-timer



Note

The **ip cef table resolution-timer** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases.

To change the Cisco Express Forwarding background resolution timer, use the **ip cef table resolution-timer** command in global configuration mode.

ip cef table resolution-timer *seconds*

no ip cef table resolution-timer *seconds*

Syntax Description

<i>seconds</i>	Timer value in seconds. Range is from 0 to 30 seconds; 0 is for the automatic exponential backoff scheme.
----------------	---

Defaults

The default configuration value is 0 seconds for automatic exponential backoff.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2SX releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Usage Guidelines

The Cisco Express Forwarding background resolution timer can use either a fixed time interval or an exponential backoff timer that reacts to the amount of resolution work required. The exponential backoff timer starts at 1 second, increasing to 16 seconds when a network flap is in progress. When the network recovers, the timer returns to 1 second.

The default is used for the exponential backoff timer. During normal operation, the default configuration value set to 0 results in re-resolution occurring much sooner than when the timer is set at a higher fixed interval.

Examples

The following example show how to set the Cisco Express Forwarding background resolution timer to 3 seconds:

```
Router(config)# ip cef table resolution-timer 3
```

ip cef traffic-statistics

To change the time interval that controls when Next Hop Resolution Protocol (NHRP) sets up or tears down a switched virtual circuit (SVC), use the **ip cef traffic-statistics** command in global configuration mode. To restore the default values, use the **no** form of this command.

ip cef traffic-statistics [**load-interval** *seconds*] [**update-rate** *seconds*]

no ip cef traffic-statistics

Syntax Description

load-interval <i>seconds</i>	(Optional) Length of time (in 30-second increments) during which the average <i>trigger-threshold</i> and <i>teardown-threshold</i> intervals are calculated before an SVC setup or teardown action is taken. (These thresholds are configured in the ip nhrp trigger-svc command.) The load-interval range is from 30 seconds to 300 seconds, in 30-second increments. The default value is 30 seconds.
update-rate <i>seconds</i>	(Optional) Frequency that the port adapter sends the accounting statistics to the Route Processor (RP). When the route processor is using NHRP in distributed Cisco Express Forwarding switching mode, this value must be set to 5 seconds. The default value is 10 seconds.

Defaults

Load interval: 30 seconds
Update rate: 10 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	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

The **ip nhrp trigger-svc** command sets the threshold by which NHRP sets up and tears down a connection. The threshold is the Cisco Express Forwarding traffic load statistics. The thresholds in the **ip nhrp trigger-svc** command are measured during a sampling interval of 30 seconds, by default. To change that interval over which that threshold is determined, use the **load-interval** *seconds* option of the **ip cef traffic-statistics** command.

When NHRP is configured on a Cisco Express Forwarding switching node with a Versatile Interface Processor (VIP2) adapter, you must make sure the **update-rate** keyword is set to 5 seconds.

Other Cisco IOS features could also use the **ip cef traffic-statistics** command; this NHRP feature relies on it.

Examples

In the following example, the triggering and teardown thresholds are calculated based on an average over 120 seconds:

```
ip cef traffic-statistics load-interval 120
```

Related Commands

Command	Description
ip nhrp trigger-svc	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

ip load-sharing

To enable load balancing for Cisco Express Forwarding, use the **ip load-sharing** command in interface configuration mode. To disable load balancing for Cisco Express Forwarding, use the **no** form of the command.

ip load-sharing [per-packet] [per-destination]

no ip load-sharing [per-packet] [per-destination]

Syntax Description

per-packet	(Optional) Enables per-packet load balancing on the interface. This functionality and keyword are not supported on all platforms. See “Usage Guidelines” for more information.
per-destination	(Optional) Enables per-destination load balancing on the interface.

Defaults

Per-destination load balancing is enabled by default when you enable Cisco Express Forwarding.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2GS	This command was introduced.
11.1CC	Multiple platform support was added.
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

Per-packet load balancing allows the router to send data packets over successive equal-cost paths without regard to individual destination hosts or user sessions. Path utilization is good, but packets destined for a given destination host might take different paths and might arrive out of order.



Note

Per-packet load balancing via Cisco Express Forwarding is not supported on Engine 2 Gigabit Switch Router (GSR) line cards (LCs).

Per-destination load balancing allows the router to use multiple, equal-cost paths to achieve load sharing. Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple, equal-cost paths are available. Traffic for different source-destination host pairs tend to take different paths.



Note

If you want to enable per-packet load sharing to a particular destination, then all interfaces that can forward traffic to the destination must be enabled for per-packet load sharing.

Cisco ASR 1000 Series Aggregation Services Routers

The **ip load-sharing** command is not supported on the Cisco ASR 1000 Series Aggregation Services Router. Per-packet load balancing is not supported. On the Cisco ASR 1000 Series Aggregation Services Router, per-destination load balancing is enabled by default and cannot be disabled.

Examples

The following example shows how to enable per-packet load balancing:

```
Router(config)# interface E0  
Router(config-if)# ip load-sharing per-packet
```

The following example shows how to enable per-destination load balancing:

```
Router(config)# interface E0  
Router(config-if)# ip load-sharing per-destination
```

Related Commands

Command	Description
ip cef	Enables CEF on the RP card.

ip route-cache

To control the use of switching methods for forwarding IP packets, use the **ip route-cache** command in interface configuration mode. To disable any of these switching methods, use the **no** form of this command.

ip route-cache [**cef** | **distributed** | **flow** | **policy** | **same-interface**]

no ip route-cache [**cef** | **distributed** | **flow** | **policy** | **same-interface**]

Syntax Description

cef	(Optional) Enables Cisco Express Forwarding operation on an interface.
distributed	(Optional) Enables distributed switching on the interface. (This keyword is not supported on the Cisco 7600 routers.) Distributed switching is disabled by default.
flow	(Optional) Enables NetFlow accounting for packets that are received by the interface. The default is disabled.
policy	(Optional) Enables fast-switching for packets that are forwarded using policy-based routing (PBR). Fast Switching for PBR (FSPBR) is disabled by default.
same-interface	(Optional) Enables fast-switching of packets onto the same interface on which they arrived.

Command Default

The switching method is not controlled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
11.1	The flow keyword was added.
11.2GS	The cef and distributed keywords were added.
11.1CC	cef keyword support was added for multiple platforms.
12.0	The policy keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The ip route-cache flow command is automatically remapped to the ip flow ingress command.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. This command is not supported on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

IP Route Cache



Note

The Cisco 10000 series routers do *not* support the **ip route-cache** command.

Using the route cache is often called *fast switching*. The route cache allows outgoing packets to be load-balanced on a *per-destination* basis rather than on a per-packet basis. The **ip route-cache** command with no additional keywords enables fast switching.

Entering the **ip route-cache** command has no effect on a subinterface. Subinterfaces accept the **no** form of the command; however, this disables Cisco Express Forwarding or distributed Cisco Express Forwarding on the physical interface and all subinterfaces associated with the physical interface.

The default behavior for Fast Switching varies by interface and media.



Note

IPv4 fast switching is removed with the implementation of the Cisco Express Forwarding infrastructure enhancements for Cisco IOS 12.2(25)S-based releases and Cisco IOS Release 12.4(20)T. For these and later Cisco IOS releases, switching path are Cisco Express Forwarding switched or process switched.

IP Route Cache Same Interface

You can enable IP fast switching when the input and output interfaces are the same interface, using the **ip route-cache same-interface** command. This configuration normally is not recommended, although it is useful when you have partially meshed media, such as Frame Relay or you are running Web Cache Communication Protocol (WCCP) redirection. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection of packets to the optimal path.

IP Route Cache Flow

The flow caching option can be used in conjunction with Cisco Express Forwarding switching to enable NetFlow, which allows statistics to be gathered with a finer granularity. The statistics include IP subprotocols, well-known ports, total flows, average number of packets per flow, and average flow lifetime.



Note

The **ip route-cache flow** command has the same functionality as the **ip flow ingress** command, which is the preferred command for enabling NetFlow. If either the **ip route-cache flow** command or the **ip flow ingress** command is configured, both commands will appear in the output of the **show running-config** command.

IP Route Cache Distributed

The distributed option is supported on Cisco routers with line cards and Versatile Interface Processors (VIPs) that support Cisco Express Forwarding switching.

On Cisco routers with Route/Switch Processor (RSP) and VIP controllers, the VIP hardware can be configured to switch packets received by the VIP with no per-packet intervention on the part of the RSP. When VIP distributed switching is enabled, the input VIP interface tries to switch IP packets instead of forwarding them to the RSP for switching. Distributed switching helps decrease the demand on the RSP.

If the **ip route-cache distributed**, **ip cef distributed**, and **ip route-cache flow** commands are configured, the VIP performs distributed Cisco Express Forwarding switching and collects a finer granularity of flow statistics.

IP Route-Cache Cisco Express Forwarding

In some instances, you might want to disable Cisco Express Forwarding or distributed Cisco Express Forwarding on a particular interface because that interface is configured with a feature that Cisco Express Forwarding or distributed Cisco Express Forwarding does not support. Because all interfaces that support Cisco Express Forwarding or distributed Cisco Express Forwarding are enabled by default when you enable Cisco Express Forwarding or distributed Cisco Express Forwarding operation globally, you must use the **no** form of the **ip route-cache distributed** command in the interface configuration mode to turn Cisco Express Forwarding or distributed Cisco Express Forwarding operation off a particular interface.

Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding on an interface disables Cisco Express Forwarding or distributed Cisco Express Forwarding switching for packets forwarded to the interface, but does not affect packets forwarded out of the interface.

Additionally, when you disable distributed Cisco Express Forwarding on the RSP, Cisco IOS software switches packets using the next-fastest switch path (Cisco Express Forwarding).

Enabling Cisco Express Forwarding globally disables distributed Cisco Express Forwarding on all interfaces. Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding globally enables process switching on all interfaces.



Note

On the Cisco 12000 series Internet router, you must not disable distributed Cisco Express Forwarding on an interface.

IP Route Cache Policy

If Cisco Express Forwarding is already enabled, the **ip route-cache route** command is not required because PBR packets are Cisco Express Forwarding-switched by default.

Before you can enable fast-switched PBR, you must first configure PBR.

FSPBR supports all of PBR's **match** commands and most of PBR's **set** commands, with the following restrictions:

- The **set ip default next-hop** and **set default interface** commands are not supported.
- The **set interface** command is supported only over point-to-point links, unless a route cache entry exists using the same interface specified in the **set interface** command in the route map. Also, at the process level, the routing table is consulted to determine if the interface is on a reasonable path to the destination. During fast switching, the software does not make this check. Instead, if the packet matches, the software blindly forwards the packet to the specified interface.



Note

Not all switching methods are available on all platforms. Refer to the *Cisco Product Catalog* for information about features available on the platform you are using.

Examples

Configuring Fast Switching and Disabling Cisco Express Forwarding Switching

The following example shows how to enable fast switching and disable Cisco Express Forwarding switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache
```

The following example shows that fast switching is enabled:

```
Router# show ip interface fastEthernet 0/0/0
```

```

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Distributed switching is disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  IP multicast fast switching is enabled

```

The following example shows that Cisco Express Forwarding switching is disabled:

```
Router# show cef interface fastEthernet 0/0/0
```

```

FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP CEF switching disabled
  IP Feature Fast switching turbo vector
  IP Null turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500

```

The following example shows the configuration information for FastEthernet interface 0/0/0:

```
Router# show running-config
```

```

.
.
!
interface FastEthernet0/0/0
  ip address 10.1.1.254 255.255.255.0
  no ip route-cache cef
  no ip route-cache distributed
!

```

The following example shows how to enable Cisco Express Forwarding (and to disable distributed Cisco Express Forwarding if it is enabled):

```
Router(config-if)# ip route-cache cef
```

The following example shows how to enable VIP distributed Cisco Express Forwarding and per-flow accounting on an interface (regardless of the previous switching type enabled on the interface):

```
Router(config)# interface e0
Router(config-if)# ip address 10.252.245.2 255.255.255.0
Router(config-if)# ip route-cache distributed
Router(config-if)# ip route-cache flow
```

The following example shows how to enable Cisco Express Forwarding on the router globally (which also disables distributed Cisco Express Forwarding on any interfaces that are running distributed Cisco Express Forwarding), and disable Cisco Express Forwarding (which enables process switching) on Ethernet interface 0:

```
Router(config)# ip cef
Router(config)# interface e0
Router(config-if)# no ip route-cache cef
```

The following example shows how to enable distributed Cisco Express Forwarding operation on the router (globally), and disable Cisco Express Forwarding operation on Ethernet interface 0:

```
Router(config)# ip cef distributed
Router(config)# interface e0
Router(config-if)# no ip route-cache cef
```

The following example shows how to reenabling distributed Cisco Express Forwarding operation on Ethernet interface 0:

```
Router(config)# ip cef distributed
Router(config)# interface e0
Router(config-if)# ip route-cache distributed
```

Configuring Fast Switching for Traffic That Is Received and Transmitted over the Same Interface

The following example shows how to enable fast switching and disable Cisco Express Forwarding switching:

```
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache same-interface
```

The following example shows that fast switching on the same interface is enabled for interface fastEthernet 0/0/0:

```
Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.224
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
```

```

ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Flow switching is disabled
IP Distributed switching is disabled
IP Feature Fast switching turbo vector
IP Null turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
IP multicast multilayer switching is disabled

```

The following example shows the configuration information for FastEthernet interface 0/0/0:

```

Router# show running-config
.
.
!
interface FastEthernet0/0/0
 ip address 10.1.1.254 255.255.255.0
 ip route-cache same-interface
 no ip route-cache cef
 no ip route-cache distributed
!

```

Enabling NetFlow Accounting

The following example shows how to enable NetFlow switching:

```

Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache flow

```

The following example shows that NetFlow accounting is enabled for FastEthernet interface 0/0/0:

```

Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
 Internet address is 10.1.1.254/24
 Broadcast address is 255.255.255.224
 Address determined by non-volatile memory
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled

```

```

IP fast switching on the same interface is disabled
IP Flow switching is enabled
IP Distributed switching is disabled
IP Flow switching turbo vector
IP Null turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, Flow
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
IP multicast multilayer switching is disabled

```

Configuring Distributed Switching

The following example shows how to enable distributed switching:

```

Router(config)# ip cef distributed
Router(config)# interface ethernet 0/0/0
Router(config-if)# ip route-cache distributed

```

The following example shows that distributed Cisco Express Forwarding switching is for FastEthernet interface 0/0/0:

```

Router# show cef interface fastEthernet 0/0/0

FastEthernet0/0/0 is up (if_number 3)
  Corresponding hwidb fast_if_number 3
  Corresponding hwidb firstsw->if_number 3
  Internet address is 10.1.1.254/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet0/0/0
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 1(1)
  Slot 0 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A02 (0x48001A02)
  IP MTU 1500

```

Configuring Fast Switching for PBR

The following example shows how to configure a simple policy-based routing scheme and to enable FSPBR:

```

Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# route-map mypbrtag permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set ip next-hop 10.1.1.195

```

```

Router(config-route-map)# exit
Router(config)# interface fastEthernet 0/0/0
Router(config-if)# ip route-cache policy
Router(config-if)# ip policy route-map mypbrtag

```

The following example shows that FSPBR is enabled for FastEthernet interface 0/0/0:

```

Router# show ip interface fastEthernet 0/0/0

FastEthernet0/0/0 is up, line protocol is up
  Internet address is 10.1.1.254/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Distributed switching is enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Distributed, Policy, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is enabled, using route map my_pbr_tag
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  IP multicast multilayer switching is disabled

```

Related Commands

Command	Description
exit	Leaves aggregation cache mode.
ip cef	Enables Cisco Express Forwarding on the RP card.
ip cef distributed	Enables distributed Cisco Express Forwarding operation.
ip flow ingress	Configures NetFlow on a subinterface.
set default interface	Configures a default interface for PBR.
set interface	Configures a specified interface for PBR.
set ip default next-hop	Configures a default IP next hop for PBR.
show cef interface	Displays detailed Cisco Express Forwarding information for interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.
show mpoa client	Displays the routing table cache used to fast switch IP traffic.

ip route-cache policy

The **policy** keyword for the **ip route-cache** command is no longer documented as a separate command.

The information for using the **policy** keyword for the **ip route-cache** command has been incorporated into the **ip route-cache** command documentation. See the **ip route-cache** command documentation for more information.

ip verify unicast notification threshold

To configure the threshold value used to determine whether to send a Unicast Reverse Path Forwarding (RPF) drop rate notification, use the **ip verify unicast notification threshold** command in interface configuration mode. To set the notification threshold back to the default value, use the **no** form of this command.

ip verify unicast notification threshold *packets-per-second*

no ip verify unicast notification threshold

Syntax Description	<i>packets-per-second</i>	Threshold value, in packets per second, used to determine whether to send a Unicast RPF drop rate notification. The range is from 0 to 4294967295. The default is 1000.
---------------------------	---------------------------	---

Command Default	No notifications are sent.
------------------------	----------------------------

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

Command History	Release	Modification
	12.2(31)SB2	This command was introduced.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
	12.2(33)SX12	This command was integrated into Cisco IOS Release 12.2(33)SX12.

Usage Guidelines	This command configures the threshold Unicast RPF drop rate which, when exceeded, triggers a notification. Configuring a value of 0 means that any Unicast RPF packet drop triggers a notification.
-------------------------	---

Examples	The following example shows how to configure a notification threshold value of 900 on Ethernet interface 3/0:
-----------------	---

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 900
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between Unicast RPF drop rate computations.
ip verify drop-rate compute window	Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.

ip verify unicast reverse-path



Note

This command was replaced by the **ip verify unicast source reachable-via** command effective with Cisco IOS Release 12.0(15)S. The **ip verify unicast source reachable-via** command allows for more flexibility and functionality, such as supporting asymmetric routing, and should be used for any Reverse Path Forward implementation. The **ip verify unicast reverse-path** command is still supported.

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast reverse-path [*list*]

no ip verify unicast reverse-path [*list*]

Syntax Description

<i>list</i>	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)
-------------	--

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1(CC) 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3
12.1(2)T	Added ACL support using the <i>list</i> argument. Added per-interface statistics on dropped or suppressed packets.
12.0(15)S	The ip verify unicast source reachable-via command replaced this command, and the following keywords were added to the ip verify unicast source reachable-via command: allow-default , allow-self-ping , rx , and any .
12.1(8a)E	The ip verify unicast reverse-path command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	The ip verify unicast reverse-path command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(14)SX	The ip verify unicast reverse-path command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SRA	The ip verify unicast reverse-path command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip verify unicast reverse-path interface** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that are received by a router. Malformed or forged source addresses can indicate denial of service (DoS) attacks on the basis of source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to ensure that the source address appears in the Forwarding Information Base (FIB) and that it matches the interface on which the packet was received. This “look backwards” ability is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

To use Unicast RPF, enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in the router. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.



Note

It is very important for Cisco Express Forwarding to be configured globally in the router. Unicast RPF will not work without Cisco Express Forwarding.



Note

Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

The Unicast Reverse Path Forwarding feature checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the Cisco Express Forwarding table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Where to Use RPF in Your Network

Unicast RPF may be used on interfaces in which only one path allows packets from valid source networks (networks contained in the FIB). Unicast RPF may also be used in cases for which a router has multiple paths to a given network, as long as the valid networks are switched via the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an

Internet service provider (ISP) are likely to have symmetrical reverse paths. Unicast RPF may still be applicable in certain multi-homed situations, provided that optional Border Gateway Protocol (BGP) attributes such as weight and local preference are used to achieve symmetric routing.

With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

For example, routers at the edge of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. In this scenario, you should use the new form of the command, **ip verify unicast source reachable-via**, if there is a chance of asymmetrical routing.

Examples

The following example shows that the Unicast Reverse Path Forwarding feature has been enabled on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 192.168.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 192.168.200.225 255.255.255.255
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 192.168.202.128 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.0 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on Ethernet interface 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at Ethernet interface 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.255
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.

ip verify unicast source reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast source reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

```
ip verify unicast source reachable-via {any | rx [I2-src]} [allow-default] [allow-self-ping]
[access-list]
```

```
no ip verify unicast source reachable-via
```

Syntax Description		
any		Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).
rx		Examines incoming packets to determine whether the source address is in the FIB and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).
I2-src		(Optional) Enables source IPv4 and source MAC address binding.
allow-default		(Optional) Allows the use of the default route for RPF verification.
allow-self-ping		(Optional) Allows a router to ping its own interface or interfaces.
		
	Caution	Use caution when enabling the allow-self-ping keyword. This keyword opens a denial-of-service (DoS) hole.
access-list		(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)

Command Default	Unicast RPF is disabled. Source IPv4 and source MAC address binding is disabled.
------------------------	---

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

Command History	Release	Modification
	11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.
	12.1(2)T	Added access control list (ACL) support using the <i>access-list</i> argument. Added per-interface statistics on dropped or suppressed packets.

Release	Modification
12.0(15)S	This command replaced the ip verify unicast reverse-path command, and the following keywords were added: allow-default , allow-self-ping , rx , and any .
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The l2-src keyword was added to support the source IPv4 and source MAC address binding feature on platforms that support the Cisco Express Forwarding software switching path.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.



Note

It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.



Note

Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to “look backwards” is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.



Note

If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement

in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ip verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately, and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Strict Mode RPF

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via rx**.

Exists-Only (or Loose Mode) RPF

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via any**.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are “peered” with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

allow-default

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the **allow-default** keyword option will override this behavior. You must specify the **allow-default** keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

allow-self-ping

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the **allow-self-ping** keyword to enable self-pinging.



Caution

Caution should be used when enabling the **allow-self-ping** keyword because this option opens a potential DoS hole.

Using RPF in Your Network

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP are likely to have symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.

**Note**

With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

IP and MAC Address Spoof Prevention

In Release 15.0(1)M and later, you can use the **l2-src** keyword to enable source IPv4 and source MAC address binding. To disable source IPv4 and source MAC address binding, use the **no** form of the **ip verify unicast source reachable-via** command.

If an inbound packet fails this security check, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.

**Note**

The **l2-src** keyword cannot be used with the loose uRPF command, **ip verify unicast source reachable-via any** command.

Not all platforms support the **l2-src** keyword. Therefore, not all the possible keyword combinations for strict Unicast RPF in the following list will apply to your platform:

Possible keyword combinations for strict Unicast RPF include the following:

```
allow-default
allow-self-ping
l2-src
<ACL-number>
allow-default allow-self-ping
allow-default l2-src
allow-default <ACL-number>
allow-self-ping l2-src
allow-self-ping <ACL-number>
l2-src <ACL-number>
allow-default allow-self-ping l2-src
allow-default allow-self-ping <ACL-number>
allow-default l2-src <ACL-number>
allow-self-ping l2-src <ACL-number>
allow-default allow-self-ping l2-src <ACL-number>
```

Examples**Single-Homed ISP Connection with Unicast RPF**

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```
ip cef
! or "ip cef distributed" for Route Switch Processor+Versatile Interface Processor-
```

```
(RSP+VIP-) based routers.
!
interface Serial5/0/0
  description - link to upstream ISP (single-homed)
  ip address 192.168.200.225 255.255.255.252
  no ip redirects
  no ip directed-broadcasts
  no ip proxy-arp
  ip verify unicast source reachable-via
```

ACLs and Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/1/1 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0/1/1 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0/1/2 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
  ip address 192.168.200.1 255.255.255.0
  ip verify unicast source reachable-via rx 197
!
int eth0/1/2
  ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

MAC Address Binding on Software Switching Platforms Like the Cisco 7200 Series Routers

The following example shows how to enable source IPv4 and source MAC address binding on Ethernet 0/0:

```
Router# configure terminal
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip verify unicast source reachable-via rx 12-src
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.
ip cef distributed	Enables Cisco Express Forwarding on the line card.

ip verify unicast vrf

To enable Unicast Reverse Path Forwarding (Unicast RPF) verification for a specified VRF, use the **ip verify unicast vrf** command in interface configuration mode. To disable the Unicast RPF check for a VRF, use the **no** form of this command.

ip verify unicast vrf *vrf-name* {**deny** | **permit**}

no ip verify unicast vrf *vrf-name* {**deny** | **permit**}

Syntax Description	<i>vrf-name</i>	Virtual Private Network (VPN) routing and forwarding (VRF) instance name.
	deny	Specifies that traffic associated with the specified VRF is dropped after it passes the Unicast RPF verification.
	permit	Specifies that traffic associated with the specified VRF is forwarded after it passes the Unicast RPF verification.

Command Default Unicast RPF verification is disabled.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	12.0(29)S	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	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.

Usage Guidelines Unicast RPF is configured to verify that the source address is in the Forwarding Information Base (FIB). The **ip verify unicast vrf** command is configured in interface configuration mode and is enabled for each VRF. This command has **permit** and **deny** keywords that are used to determine if traffic is forwarded or dropped after Unicast RPF verification.

Examples The following example configures Unicast RPF verification for VRF1 and VRF2. VRF1 traffic is forwarded. VRF2 traffic is dropped.

```
Router(config)# interface Ethernet 0
Router(config-if)# ip verify unicast vrf vrf1 permit
Router(config-if)# ip verify unicast vrf vrf2 deny
Router(config-if)# end
```

Related Commands

Command	Description
import ipv4	Configures an import map to import IPv4 prefixes from the global routing table to a VRF table.
ip vrf	Configures a VRF routing table.
rd	Creates routing and forwarding tables for a VRF.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

ipv6 cef

To enable Cisco Express Forwarding for IPv6, use the **ipv6 cef** command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

ipv6 cef

no ipv6 cef

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding for IPv6 is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	This command was introduced.
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(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.

Usage Guidelines

The **ipv6 cef** command is similar to the **ip cef** command, except that it is IPv6-specific.

The **ipv6 cef** command is not available on the Cisco 12000 series Internet routers because this distributed platform operates only in distributed Cisco Express Forwarding for IPv6 mode.



Note

The **ipv6 cef** command is not supported in interface configuration mode.



Note

Some distributed architecture platforms, such as the Cisco 7500 series routers, support both Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6. When Cisco Express Forwarding for IPv6 is configured on distributed platforms, Cisco Express Forwarding switching is performed by the Route Processor (RP).



Note

You must enable Cisco Express Forwarding for IPv4 by using the **ip cef** global configuration command before enabling Cisco Express Forwarding for IPv6 by using the **ipv6 cef** global configuration command.

Cisco Express Forwarding for IPv6 is advanced Layer 3 IP switching technology that functions the same and offer the same benefits as Cisco Express Forwarding for IPv4. Cisco Express Forwarding for IPv6 optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables standard Cisco Express Forwarding for IPv4 operation and then standard Cisco Express Forwarding for IPv6 operation globally on the router.

```
ip cef
ipv6 cef
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
ipv6 cef accounting	Enables Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting.
ipv6 cef distributed	Enables distributed Cisco Express Forwarding for IPv6.
show cef	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef accounting

To enable Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting, use the **ipv6 cef accounting** command in global configuration mode or interface configuration mode. To disable Cisco Express Forwarding for IPv6 network accounting, use the **no** form of this command.

ipv6 cef accounting *accounting-types*

no ipv6 cef accounting *accounting-types*

Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode

ipv6 cef accounting non-recursive { **external** | **internal** }

no ipv6 cef accounting non-recursive { **external** | **internal** }

Syntax Description

<i>accounting-types</i>	The <i>accounting-types</i> argument must be replaced with at least one of the following keywords. Optionally, you can follow this keyword by any or all of the other keywords, but you can use each keyword only once.
	• load-balance-hash—Enables load balancing hash bucket counters. • non-recursive—Enables accounting through nonrecursive prefixes. • per-prefix—Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix). • prefix-length—Enables accounting through prefix length.
non-recursive	Enables accounting through nonrecursive prefixes. This keyword is optional when used in global configuration mode after another keyword is entered. See the <i>accounting-types</i> argument.
external	Counts input traffic in the nonrecursive external bin.
internal	Counts input traffic in the nonrecursive internal bin.

Command Default

Cisco Express Forwarding for IPv6 network accounting is disabled by default.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.0(22)S	This command was introduced.
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.

Release	Modification
12.2(25)S	The non-recursive and load-balance-hash keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **ipv6 cef accounting** command is similar to the **ip cef accounting** command, except that it is IPv6-specific.

Configuring Cisco Express Forwarding for IPv6 network accounting enables you to collect statistics on Cisco Express Forwarding for IPv6 traffic patterns in your network.

When you enable network accounting for Cisco Express Forwarding for IPv6 by using the **ipv6 cef accounting** command in global configuration mode, accounting information is collected at the Route Processor (RP) when Cisco Express Forwarding for IPv6 mode is enabled and at the line cards when distributed Cisco Express Forwarding for IPv6 mode is enabled. You can then display the collected accounting information using the **show ipv6 cef EXEC** command.

For prefixes with directly connected next hops, the **non-recursive** keyword enables express forwarding of the collection of packets and bytes through a prefix. This keyword is optional when this command is used in global configuration mode after you enter another keyword on the **ipv6 cef accounting** command.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the **show ipv6 cef detail** command.

Per-destination load balancing uses a series of 16 hash buckets into which the set of available paths are distributed. A hash function operating on certain properties of the packet is applied to select a bucket that contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the **load-balance-hash** keyword with the **ipv6 cef accounting** command to enable per-hash-bucket counters. Enter the **show ipv6 cef prefix internal** command to display the per-hash-bucket counters.

Examples

The following example enables the collection of Cisco Express Forwarding for IPv6 accounting information for prefixes with directly connected next hops:

```
Router(config)# ipv6 cef accounting non-recursive
```

Related Commands

Command	Description
ip cef accounting	Enable Cisco Express Forwarding network accounting (for IPv4).
show cef	Displays information about packets forwarded by Cisco Express Forwarding.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef distributed

To enable distributed Cisco Express Forwarding for IPv6, use the **ipv6 cef distributed** command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

ipv6 cef distributed

no ipv6 cef distributed

Syntax Description

This command has no arguments or keywords.

Command Default

Distributed Cisco Express Forwarding for IPv6 is disabled on the Cisco 7500 series routers and enabled on the Cisco 12000 series Internet routers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	This command was introduced.
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(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.

Usage Guidelines

The **ipv6 cef distributed** command is similar to the **ip cef distributed** command, except that it is IPv6-specific.

Enabling distributed Cisco Express Forwarding for IPv6 globally on the router by using the **ipv6 cef distributed** in global configuration mode distributes the Cisco Express Forwarding processing of IPv6 packets from the Route Processor (RP) to the line cards of distributed architecture platforms.



Note

The **ipv6 cef distributed** command is not supported on the Cisco 12000 series Internet routers because distributed Cisco Express Forwarding for IPv6 is enabled by default on this platform.



Note

To forward distributed Cisco Express Forwarding for IPv6 traffic on the router, configure the forwarding of IPv6 unicast datagrams globally on your router by using the **ipv6 unicast-routing** global configuration command, and configure an IPv6 address and IPv6 processing on an interface by using the **ipv6 address** interface configuration command.



Note

You must enable distributed Cisco Express Forwarding for IPv4 by using the **ip cef distributed** global configuration command before enabling distributed Cisco Express Forwarding for IPv6 by using the **ipv6 cef distributed** global configuration command.

Cisco Express Forwarding is advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables distributed Cisco Express Forwarding for IPv6 operation:

```
ipv6 cef distributed
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv6, use the **ipv6 cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

```

ipv6 cef load-sharing algorithm { original | universal [id] | include-ports { source [id] |
[destination] [id] | source [id] destination [id] } }

```

```

no ipv6 cef load-sharing algorithm

```

Syntax Description		
original		Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.
universal		Sets the load-balancing algorithm to the universal algorithm that uses a source and destination and an ID hash.
<i>id</i>		(Optional) Fixed identifier in hexadecimal format.
include-ports source		Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 source port.
include-ports destination		Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 destination port.
include-ports source destination		Sets the load balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.

Command Default The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

Command Modes Global configuration (config)

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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	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.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **ipv6 cef load-sharing algorithm** command is similar to the **ip cef load-sharing algorithm** command, except that it is IPv6-specific.

When the Cisco Express Forwarding for IPv6 load-balancing algorithm is set to universal mode, each router on the network can make a different load-sharing decision for each source-destination address pair.

The include-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not load-shared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

Examples

The following example shows how to enable the Cisco Express Forwarding load-balancing algorithm for IPv6 for Layer-4 source and destination ports:

```
Router(config)# ipv6 cef load-sharing algorithm include-ports source destination
```

The router automatically generates fixed IDs for the algorithm.

Related Commands

Command	Description
debug ipv6 cef hash	Displays debug messages for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 load-sharing hash algorithm events.
ip cef load-sharing algorithm	Selects a Cisco Express Forwarding load-balancing algorithm (for IPv4).

ipv6 cef optimize neighbor resolution

To configure address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **ipv6 cef optimize neighbor resolution** command in global configuration mode. To disable address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **no** form of this command.

ipv6 cef optimize neighbor resolution

no ipv6 cef optimize neighbor resolution

Syntax Description This command has no arguments or keywords.

Command Default If this command is not configured, Cisco Express Forwarding for IPv6 does not optimize the address resolution of directly connected neighbors.

Command Modes Global configuration (config)

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 The **ipv6 cef optimize neighbor resolution** command is very similar to the **ip cef optimize neighbor resolution** command, except that it is IPv6-specific.

Use this command to trigger Layer 2 address resolution of neighbors directly from Cisco Express Forwarding for IPv6.

Examples The following example shows how to optimize address resolution from Cisco Express Forwarding for IPv6 for directly connected neighbors:

```
Router(config)# ipv6 cef optimize neighbor resolution
```

Related Commands	Command	Description
	ip cef optimize neighbor resolution	Configures address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors.

ipv6 verify unicast reverse-path

To enable Unicast Reverse Path Forwarding (Unicast RPF) for IPv6, use the **ipv6 verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ipv6 verify unicast reverse-path [**access-list** *name*]

no ipv6 verify unicast reverse-path [**access-list** *name*]

Syntax Description

access-list <i>name</i>	(Optional) Specifies the name of the access list.
Note	This keyword and argument are not supported on the Cisco 12000 series Internet router.

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S and introduced on the 10G Engine 5 SPA Interface Processor in the Cisco 12000 series Internet router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in strict checking mode. The Unicast RPF for IPv6 feature requires that Cisco Express Forwarding for IPv6 is enabled on the router.



Note

Beginning in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both the **ipv6 verify unicast reverse-path** and **ipv6 verify unicast source reachable-via rx** commands to enable Unicast RPF to be compatible with the Cisco IOS Release 12.3T and 12.2S software trains.

Use the **ipv6 verify unicast reverse-path** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source IPv6 address appears in the routing table and that it is reachable by a path through the interface on which the packet was received. Unicast RPF is an input feature and is applied only on the input interface of a router at the upstream end of a connection.

The Unicast RPF feature performs a reverse lookup in the CEF table to check if any packet received at a router interface has arrived on a path identified as a best return path to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast RPF command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast RPF command. Log information can be used to gather information about the attack, such as source address, time, and so on.



Note

When you configure Unicast RPF for IPv6 on the Cisco 12000 series Internet router, the most recently configured checking mode is not automatically applied to all interfaces as on other platforms. You must enable Unicast RPF for IPv6 separately on each interface.

When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format *slot/subslot/port*.

The optional **access-list** keyword for the **ipv6 verify unicast reverse-path** command is not supported on the Cisco 12000 series Internet router. For information about how Unicast RPF can be used with ACLs on other platforms to mitigate the transmission of invalid IPv4 addresses (perform egress filtering) and to prevent (deny) the reception of invalid IPv4 addresses (perform ingress filtering), refer to the “Configuring Unicast Reverse Path Forwarding” chapter in the “Other Security Features” section of the *Cisco IOS Security Configuration Guide*.



Note

When using Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on).

Do not use Unicast RPF on core-facing interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Apply Unicast RPF only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (ISP) are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Examples

Unicast Reverse Path Forwarding on a Serial Interface

The following example shows how to enable the Unicast RPF feature on a serial interface:

```
interface serial 5/0/0
  ipv6 verify unicast reverse-path
```

Unicast Reverse Path Forwarding on a Cisco 12000 Series Internet Router

The following example shows how to enable Unicast RPF for IPv6 with strict checking on a 10G SIP Gigabit Ethernet interface 2/1/2:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# interface gigabitEthernet 2/1/2

Router(config-if)# ipv6 verify unicast reverse-path
Router(config-if)# exit
```

Unicast Reverse Path Forwarding on a Single-Homed ISP

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
interface Serial 5/0/0
description Connection to Upstream ISP
ipv6 address FE80::260:3EFF:FE11:6770/64
no ipv6 redirects
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 host 2::1 any
deny ipv6 FEC0::/10 any
    ipv6 access-group abc in
    ipv6 access-group jkl out
!
access-list abc permit ip FE80::260:3EFF:FE11:6770/64 2001:0DB8:0000:0001::0001 any
access-list abc deny ipv6 any any log
access-list jkl deny ipv6 host 2001:0DB8:0000:0001::0001 any log
access-list jkl deny ipv6 2001:0DB8:0000:0001:FFFF:1234::5 255.255.255 any log
access-list jkl deny ipv6 2002:0EF8:002001:0DB8:0000:0001:FFFF:1234::5 172.16.0.0
0.15.255.255 any log
access-list jkl deny ipv6 2001:0CB8:0000:0001:FFFF:1234::5 0.0.255.255 any log
access-list jkl deny ipv6 2003:0DB8:0000:0001:FFFF:1234::5 0.0.0.31 any log
access-list jkl permit ipv6
```

ACL Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL abc provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/0 to check packets arriving at that interface.

For example, packets with a source address of 8765:4321::1 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL “abc.” In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 1234:5678::1 arriving at Ethernet interface 0/0 are forwarded because of the permit statement in ACL abc. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
interface ethernet 0/0
ipv6 address FE80::260:3EFF:FE11:6770/64 link-local
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
```

```
permit ipv6 1234:5678::/64 any log-input
deny ipv6 8765:4321::/64 any log-input
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.
ip verify unicast reverse-path	Enables Unicast RPF for IPv4 traffic.
ipv6 cef	Enables Cisco Express Forwarding for IPv6 interfaces.

ipv6 verify unicast source reachable-via

To verify that a source address exists in the FIB table and enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ipv6 verify unicast source reachable-via** command in interface configuration mode. To disable URPF, use the **no** form of this command.

```

ipv6 verify unicast source reachable-via { rx | any } [allow-default] [allow-self-ping]
    [access-list-name]
  
```

```

no ipv6 verify unicast
  
```

Syntax Description	rx	Source is reachable through the interface on which the packet was received.
	any	Source is reachable through any interface.
	allow-default	(Optional) Allows the lookup table to match the default route and use the route for verification.
	allow-self-ping	(Optional) Allows the router to ping a secondary address.
	<i>access-list-name</i>	(Optional) Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeral.

Command Default Unicast RPF is disabled.

Command Modes Interface configuration (config-if)

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.
	Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in loose checking mode.

Use the **ipv6 verify unicast source reachable-via** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through an IPv6 router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing.

The URPF feature checks to see if any packet received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the CEF table. If URPF does not find a reverse path for the packet, U RPF can drop or forward the packet, depending on whether an access control list (ACL) is specified in the **ipv6 verify unicast source reachable-via** command. If an ACL is specified in the command, then when (and only when) a packet fails the URPF check, the ACL is checked to see if the packet should be dropped (using a deny statement in the ACL)

or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for U RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ipv6 verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

U RPF events can be logged by specifying the logging option for the ACL entries used by the **ipv6 verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Examples

The following example enables Unicast RPF on any interface:

```
ipv6 verify unicast source reachable-via any
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

mls cef maximum-routes

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

mls cef maximum-routes { **ip** | **ip-multicast** | **ipv6** | **mpls** } *maximum-routes*

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

Syntax Description

ip	Specifies the maximum number of IP routes.
<i>maximum-routes</i>	Maximum number of the routes that can be programmed in the hardware allowed per protocol.
ip-multicast	Specifies the maximum number of multicast routes.
ipv6	Specifies the maximum number of IPv6 routes.
mpls	Specifies the maximum number of Multiprotocol Label Switching (MPLS) labels.

Command Default

The defaults are as follows:

- For XL-mode systems:
 - IPv4 unicast and MPLS—512,000 routes
 - IPv6 unicast and IPv4 multicast—256,000 routes
- For non-XL mode systems:
 - IPv4 unicast and MPLS—192,000 routes
 - IPv6 unicast and IPv4 multicast—32,000 routes



Note

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17b)SXA	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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines



Note

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

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

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

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

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

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

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

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

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



Note

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

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

```
mls cef maximum-routes ip 4
```

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

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

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

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

Examples

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

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

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

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

Related Commands

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

mls cef tunnel fragment

To allow tunnel fragmentation, use the **mls cef tunnel fragment** command. To return to the default settings, use the **no** form of this command.

mls cef tunnel fragment

no mls cef tunnel fragment

Syntax Description This command has no arguments or keywords.

Command Default Tunnel fragmentation is not enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(18)SXF	This command was introduced.
	12.2(33)SXH	This command was modified. Support was added for PCF3BXL, PFC3C, and PFC3CXL modes only.
	12.2(33)SXI	This command was modified. Support was added for PCF3BXL, PFC3C, and PFC3CXL modes only.
	12.2(33)SXI2	This command was modified. Support was added for all PFC3 modes.

Usage Guidelines When you enable tunnel fragmentation, if the size of the packets that are going into a tunnel interface exceed the MTU, the packet is fragmented. The packets that are fragmented are reassembled at the destination point.

Examples This example shows how to allow tunnel fragmentation:

```
Router(config)# mls cef tunnel fragment
```

This example shows how to return to the default setting:

```
Router(config)# no mls cef tunnel fragment
```

Related Commands	Command	Description
	show mls cef tunnel fragment	Displays the operational status of tunnel fragmentation.

mls erm priority

To assign the priorities to define an order in which protocols attempt to recover from the exception status, use the **mls erm priority** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls erm priority *ipv4 value ipv6 value mpls value*

no mls erm priority *ipv4 value ipv6 value mpls value*

Syntax Description

ipv4	Prioritizes the IPv4 protocol. The default priority is 1.
<i>value</i>	Priority value; valid values are from 1 to 3.
ipv6	Prioritizes the IPv6 protocol. The default priority is 2.
mpls	Prioritizes the Multiprotocol Label Switching (MPLS) protocol. The default priority is 3.

Command Default

The default priority settings are used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to support the ipv6 keyword.
12.2(17b)SXA	This command was changed to support the mpls keyword.
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.

A lower *value* indicates a higher priority.

When a protocol sees a Forwarding Information Base (FIB) table exception, the protocol notifies the FIB Embedded Resource Manager (ERM). The FIB ERM periodically polls the FIB table exception status and decides which protocol gets priority over another protocol when multiple protocols are running under the exception. Only one protocol can attempt to recover from an exception at any time.

If there is sufficient FIB space, the protocol with the highest priority tries to recover first. Other protocols under the exception do not start to recover until the previous protocol completes the recovery process by reloading the appropriate FIB table.

Examples

This example shows how to set the ERM exception-recovery priority:

```
Router(config)# mls erm priority ipv4 2 ipv6 1 mpls 3
```

This example shows how to return to the default setting:

```
Router(config)# no mls erm priority ipv4 2 ipv6 1 mpls 3
```

Related Commands

Command	Description
show mls cef exception	Displays information about the Cisco Express Forwarding exception.

mls ip

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

mls ip

no mls ip

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Multicast is disabled.
-----------------	------------------------

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

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

Examples	This example shows how to enable MLS IP:
-----------------	--

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

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

mls ip cef accounting per-prefix

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

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

no mls ip cef accounting per-prefix

Syntax Description	<i>prefix-entry</i>	Prefix entry in the format A.B.C.D.
	<i>prefix-entry-mask</i>	Prefix entry mask in the format A.B.C.D.
	<i>instance-name</i>	(Optional) Virtual Private Network (VPN) routing and forwarding instance name.

Command Default MLS per-prefix accounting is disabled by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(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(18)SXF	Support for this command was implemented on the Supervisor Engine 32.

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

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

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

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

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

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

mls ip cef load-sharing

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

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

no mls ip cef load-sharing
```

Syntax Description

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

Defaults

Source and destination IP address and universal identification

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was introduced in Release 12.2(17d)SXB.
12.2(17d)SXB2	This command was changed as follows: - The simple keyword was added. - Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to include the exclude-port , destination , and source keywords on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

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

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

This example shows how to return to the default setting:

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

Related Commands

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

mls ip cef rate-limit

To rate-limit Cisco Express Forwarding-punted data packets, use the **mls ip cef rate-limit** command in global configuration mode. To disable the rate-limited Cisco Express Forwarding-punted data packets, use the **no** form of this command.

mls ip cef rate-limit *packets-per-second*

no mls ip cef rate-limit

Syntax Description

packets-per-second Number of data packets per second; see the “Usage Guidelines” section for the valid values.

Defaults

No rate limit is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The valid values for the number of data packets per second are as follows:

- For Cisco 7600 series routers that are configured with a Supervisor Engine 2, the valid values are from 1 to 1000000.
- For Cisco 7600 series routers that are configured with a Supervisor Engine 720, the valid values are from 0 to 1000000.

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

This command rate limits all Cisco Express Forwarding-punted data packets including the following:

- Data packets going to the local interface IP address
- Data packets requiring Address Resolution Protocol (ARP)

Setting the rate to a low value could impact the packets that are destined to the IP addresses of the local interfaces and the packets that require ARP.

You should use this command to limit these packets to a normal rate and to avoid abnormal incoming rates.

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

Examples

This example shows how to enable and set rate limiting:

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

Related Commands

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

mls ip cef rpf hw-enable-rpf-acl

To enable hardware unicast Reverse Path Forwarding (uRPF) for packets matching the deny Access Control List (ACL) when uRPF with ACL is enabled, use the **mls ip cef rpf hw-enable-rpf-acl** command in global configuration mode. To disable hardware uRPF when RPF and ACL are enabled, use the **no** form of this command.

mls ip cef rpf hw-enable-rpf-acl

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

Syntax Description This command has no arguments or keywords.

Command Default uRPF is disabled.

Command Modes Global configuration (config)

Release	Modification
12.2(18)SXF6	This command was introduced.

Usage Guidelines This command is supported on systems configured with a PFC3 (Supervisor Engine 720 and Supervisor Engine 32) only.

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

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

```
mls ip cef rpf hw-enable-rpf-acl
```

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

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

Command	Description
ip verify unicast source reachable-via	Enables and configures RPF checks with ACL.

mls ip cef rpf interface-group

To define an interface group in the Reverse Path Forwarding (RPF)-VLAN table, use the **mls ip cef rpf interface-group** command in global configuration mode. To delete the interface group, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

No groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(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.

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

Enter the *interface* as *interface-type**mod/port*.

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

Examples

This example shows how to define an interface group:

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

mls ip cef rpf multipath

To configure the Reverse Path Forwarding (RPF) modes, use the **mls ip cef rpf multipath** command in global configuration mode. To return to the default settings, use the **no** form of this command.

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

no mls ip cef rpf multipath {interface-group | punt | pass}

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

Defaults	punt
-----------------	-------------

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

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(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 interface-group mode is similar to the pass mode but utilizes the RPF_VLAN global table for the RPF check. Packets from other multiple path prefixes always pass the RPF check.
	You enter the mls ip cef rpf multipath interface-group command to define an RPF_VLAN table interface group. One interface group contains from three to six interfaces, and you can configure up to four interface groups. For each interface group, the first four entries are installed in the hardware RPF_VLAN table. For the prefix that has more than three multiple paths, and all paths except two are part of that interface group, the FIB entry of that prefix uses this RPF_VLAN entry.

Examples	This example shows how to redirect the RPF-failed packets to the route processor for multiple path prefix support:
	Router(config)# mls ip cef rpf multipath interface-group

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

monitor event-trace (EXEC)

To monitor and control the event trace function for a specified Cisco IOS software subsystem component, use the **monitor event-trace** command in privileged EXEC mode.

monitor event-trace *component* { **clear** | **continuous** | **disable** | **dump** [**pretty**] | **enable** | **one-shot** }

Cisco 10000 Series Routers

monitor event-trace *component* { **disable** | **dump** | **enable** | **size** | **stacktrace** }

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

monitor event-trace all-traces { **continuous** [**cancel**] | **dump** [**merged**] [**pretty**] }

monitor event-trace l3 { **clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **interface** *type mod/port* | **one-shot** }

monitor event-trace spa { **clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot** }

monitor event-trace subsys { **clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot** }

Syntax Description

<i>component</i>	Name of the Cisco IOS software subsystem component that is the subject of the event trace. To get a list of components that support event tracing, use the monitor event-trace ? command.
clear	Clears existing trace messages for the specified component from memory on the networking device.
continuous	Continuously displays the latest event trace entries.
disable	Turns off event tracing for the specified component.
dump	Writes the event trace results to the file configured using the monitor event-trace command in global configuration mode. The trace messages are saved in binary format.
pretty	(Optional) Saves the event trace message in ASCII format.
enable	Turns on event tracing for the specified component.
one-shot	Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the monitor event-trace command in global configuration mode.
size	Sets the number of messages that can be written to memory for a single instance of a trace. Note Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the show monitor event-trace component parameters command. When the number of event trace messages in memory exceeds the size, new messages will begin to overwrite the older messages in the file.
stacktrace	Enables the stack trace at tracepoints.
all-traces	Displays the configured merged-event traces.

merged	(Optional) Dumps the entries in all event traces sorted by time.
l3	Displays information about the Layer 3 trace.
spa	Displays information about the Shared Port Adapter (SPA) trace.
interface type mod/port	Specifies the interface to be logged.
cancel	(Optional) Cancels the continuous display of latest trace entries.
subsys	Displays information about the subsystem's initial trace.

Command Default

The event trace function is disabled by default.

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(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The monitor event-trace cef ipv4 clear command replaces the clear ip cef event-log command.
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 **monitor event-trace** command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace** command in global configuration mode.

**Note**

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace** command in global configuration mode for each instance of a trace.

The Cisco IOS software allows for the subsystem components to define whether support for event tracing is enabled or disabled at boot time. You can enable or disable event tracing in two ways: using the **monitor event-trace** command in privileged EXEC mode or using the **monitor event-trace** command in global configuration mode. To disable event tracing, you would enter either of these commands with the **disable** keyword. To enable event tracing again, you would enter either of these commands with the **enable** keyword.

To determine whether you can enable event tracing on a subsystem, use the **monitor event-trace ?** command to get a list of software components that support event tracing. To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to display trace messages.

Use the **show monitor event-trace** command to display trace messages. Use the **monitor event-trace component dump** command to save trace message information for a single event. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace component dump pretty** command.

To write the trace messages for all events currently enabled on a networking device to a file, enter the **monitor event-trace dump** command.

To configure the file where you want to save trace information, use the **monitor event-trace** command in global configuration mode. The trace messages are saved in a binary format.

Examples

The following example shows the privileged EXEC commands to stop event tracing, clear the current contents of memory, and reenables the trace function for the interprocess communication (IPC) component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace ipc disable
Router# monitor event-trace ipc clear
Router# monitor event-trace ipc enable
```

The following example shows how the **monitor event-trace one-shot** command accomplishes the same function as the previous example except in one command. In this example, once the size of the trace message file has been exceeded, the trace is terminated.

```
Router# monitor event-trace ipc one-shot
```

The following example shows the command for writing trace messages for an event in binary format. In this example, the trace messages for the IPC component are written to a file.

```
Router# monitor event-trace ipc dump
```

The following example shows the command for writing trace messages for an event in ASCII format. In this example, the trace messages for the MBUS component are written to a file.

```
Router# monitor event-trace mbus dump pretty
```

Catalyst 6500 Series Switches and Cisco 7600 Series Routers Examples Only

This example shows how to stop event tracing, clear the current contents of memory, and reenables the trace function for the SPA component. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace spa disable
Router# monitor event-trace spa clear
Router# monitor event-trace spa enable
```

Related Commands

Command	Description
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	Displays event trace messages for Cisco IOS software subsystem components.

monitor event-trace (global)

To configure event tracing for a specified Cisco IOS software subsystem component, use the **monitor event-trace** command in global configuration mode.

monitor event-trace *component* { **disable** | **dump-file** *filename* | **enable** | **size** *number* | **stacktrace** *number* }

monitor event-trace timestamps [**datetime** [**localtime**] [**msec**] [**show-timezone**] | **uptime**]

Cisco 10000 Series Routers

monitor event-trace *component* { **disable** | **dump-file** *filename* | **enable** | **clear** | **continuous** | **one-shot** }

Syntax Description		
<i>component</i>		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, use the monitor event-trace ? command.
disable		Turns off event tracing for the specified component.
dump-file <i>filename</i>		Specifies the file where event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
enable		Turns on event tracing for the specified component provided that the component has been configured using the monitor event-trace command.
size <i>number</i>		Sets the number of messages that can be written to memory for a single instance of a trace. Valid values are from 1 to 65536.
	Note	Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the show monitor event-trace component parameters command.
		When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace <i>number</i>		Enables the stack trace at tracepoints and specifies the depth of the stack trace stored. Valid values are from 1 to 16.
timestamps		Includes time stamp information with the event trace messages for the specified component.
datetime		(Optional) Specifies that the time stamp information included with event trace messages will consist of the date and time of the event trace.
localtime		(Optional) Specifies that the time given in the time stamp will be local time.
msec		(Optional) Includes milliseconds in the time stamp.
show-timezone		(Optional) Includes time zone information in the time stamp.
uptime		(Optional) Displays time stamped information about the system uptime.
clear		Clears existing trace messages for the specified component from memory on the networking device.

continuous	Continuously displays the latest event trace entries.
one-shot	Clears any existing trace information from memory, starts event tracing again, and disables the trace when the trace reaches the size specified using the monitor event-trace command.

Command Default

Event tracing is enabled or disabled depending on the software component.

Command Modes

Global configuration (config)

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(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on the Supervisor Engine 720.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **monitor event-trace** command to enable or disable event tracing and to configure event trace parameters for Cisco IOS software subsystem components.

**Note**

Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a Technical Assistance Center (TAC) representative. In Cisco IOS software images that do not provide subsystem support for the event trace function, the **monitor event-trace** command is not available.

The Cisco IOS software allows the subsystem components to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default two ways: using the **monitor event-trace** command in privileged EXEC mode or using the **monitor event-trace** command in global configuration mode.

Additionally, default settings do not show up in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace component enable** command will not show up in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a command entry in the configuration file.

**Note**

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace** command for each instance of a trace.

To determine whether you can enable event tracing on a subsystem, use the **monitor event-trace ?** command to get a list of software components that support event tracing.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace** command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for the interprocess communication (IPC) subsystem component in Cisco IOS software and configure the size to 4096 messages. The trace messages file is set to ipc-dump in slot0 (flash memory).

```
configure terminal
!
monitor event-trace ipc enable
monitor event-trace ipc dump-file slot0:ipc-dump
monitor event-trace ipc size 4096
```

When you select Cisco Express Forwarding as the component for which to enable event tracing, you can use the following additional arguments and keywords: **monitor event-trace cef** [**events** | **interface** | **ipv6** | **ipv4**][**all**]. The following example shows how to enable event tracing for IPv4 or IPv6 events of the Cisco Express Forwarding component in Cisco IOS software:

```
configure terminal
!
monitor event-trace cef ipv4 enable

configure terminal
!
monitor event-trace cef ipv6 enable
exit
```

The following example shows what happens when you try to enable event tracing for a component (in this case, adjacency events) when it is already enabled:

```
configure terminal
!
monitor event-trace adjacency enable

%EVENT_TRACE-6-ENABLE: Trace already enabled.
```

Related Commands

Command	Description
monitor event-trace (EXEC)	Controls the event trace function 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	Displays event trace messages for Cisco IOS software subsystem components.

monitor event-trace cef (EXEC)

To monitor and control the event trace function for Cisco Express Forwarding, use the **monitor event-trace cef** command in privileged EXEC mode.

```
monitor event-trace cef { dump [merged pretty | pretty] | { events | interface | ipv4 | ipv6 } { clear  
| continuous [cancel] | disable | dump [pretty] | enable | one-shot } }
```

Syntax Description		
dump		Writes the event trace results to the file configured with the global configuration monitor event-trace cef command. The trace messages are saved in binary format.
merged pretty		(Optional) Sorts all event trace entries by time and writes the entries to a file in ASCII format.
pretty		(Optional) Saves the event trace message in ASCII format.
events		Monitors Cisco Express Forwarding events.
interface		Monitors Cisco Express Forwarding interface events.
ipv4		Monitors Cisco Express Forwarding IPv4 events.
ipv6		Monitors Cisco Express Forwarding IPv6 events.
clear		Clears existing trace messages for Cisco Express Forwarding from memory on the networking device.
continuous		Continuously displays the latest event trace entries.
cancel		(Optional) Cancels the continuous display of the latest trace entries.
disable		Turns off Cisco Express Forwarding event tracing.
enable		Turns on Cisco Express Forwarding event tracing.
one-shot		Clears any existing trace information from memory, starts event tracing again, and disables the trace when the size of the trace message file configured in the global configuration command is exceeded.

Command Default Event tracing for Cisco Express Forwarding is enabled by default.

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(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)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.
	12.2(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.

Release	Modification
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **monitor event-trace cef** command to control what, when, and how Cisco Express Forwarding event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace cef** command in global configuration mode.



Note

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef** command in global configuration mode for each instance of a trace.

You can enable or disable Cisco Express Forwarding event tracing in one of two ways: using the **monitor event-trace cef** command in privileged EXEC mode or using the **monitor event-trace cef** command in global configuration mode. To disable event tracing, you would enter either of these commands with the **disable** keyword. To enable event tracing again, you would enter either of these commands with the **enable** keyword.

Use the **show monitor event-trace cef** command to display trace messages. Use the **monitor event-trace cef dump** command to save trace message information for a single event. By default, trace information is saved in binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace cef dump pretty** command.

To configure the file in which you want to save trace information, use the **monitor event-trace cef** command in global configuration mode. The trace messages are saved in a binary format.

Examples

The following example shows the privileged EXEC commands that stop event tracing, clear the current contents of memory, and reenables the trace function for Cisco Express Forwarding events. This example assumes that the tracing function is configured and enabled on the networking device.

```
Router# monitor event-trace cef events disable
Router# monitor event-trace cef events clear
Router# monitor event-trace cef events enable
```

The following example shows how to configure the continuous display of the latest Cisco Express Forwarding event trace entries for IPv4 events:

```
Router# monitor event-trace cef ipv4 continuous
```

The following example shows how to stop the continuous display of the latest trace entries:

```
Router# monitor event-trace cef ipv4 continuous cancel
```

Related Commands

Command	Description
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.
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.

monitor event-trace cef (global)

To configure event tracing for Cisco Express Forwarding, use the **monitor event-trace cef** command in global configuration mode. To disable event tracing for Cisco Express Forwarding, use the **no** form of this command.

monitor event-trace cef { **dump-file** *dump-file-name* | { **events** | **interface** } { **disable** | **dump-file** *dump-file-name* | **enable** | **size** *number* | **stacktrace** [*depth*] } }

no monitor event-trace cef { **dump-file** *dump-file-name* | { **events** | **interface** } { **disable** | **dump-file** *dump-file-name* | **enable** | **size** | **stacktrace** [*depth*] } }

Syntax Description

dump-file <i>dump-file-name</i>	Specifies the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
events	Turns on event tracing for Cisco Express Forwarding events.
interface	Turns on event tracing for Cisco Express Forwarding interface events.
disable	Turns off event tracing for Cisco Express Forwarding events.
enable	Turns on event tracing for Cisco Express Forwarding events if it had been enabled with the monitor event-trace cef command.
size <i>number</i>	Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536. Note Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the show monitor event-trace cef parameters command. When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace	Enables the stack trace at tracepoints.
<i>depth</i>	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.

Command Default

Event tracing for Cisco Express Forwarding is enabled by default.

Command Modes

Global configuration (config)

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.

Release	Modification
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **monitor event-trace cef** command to enable or disable event tracing and to configure event trace parameters for Cisco Express Forwarding.

The Cisco IOS software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef** command in privileged EXEC mode or using the **monitor event-trace cef** command in global configuration mode.

Additionally, default settings do not appear in the configuration file. If Cisco Express Forwarding enables event tracing by default, the **monitor event-trace cef enable** command does not appear in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem creates a command entry in the configuration file.



Note

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef** command for each instance of a trace.

To determine whether event tracing is enabled by default for Cisco Express Forwarding, use the **show monitor event-trace cef** command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for Cisco Express Forwarding and configure the buffer size to 5000 messages. The trace messages file is set to cef-dump in slot0 (flash memory).

```
Router(config)# monitor event-trace cef events enable

Router(config)# monitor event-trace cef dump-file slot0:cef-dump

Router(config)# monitor event-trace cef events size 5000
```

The following example shows what happens when you try to enable event tracing for Cisco Express Forwarding events when it is already enabled:

```
Router(config)# monitor event-trace cef events enable

Router(config)#
00:04:33: %EVENT_TRACE-6-ENABLE: Trace already enabled.
```

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function 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.
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.

monitor event-trace cef ipv4 (global)

To configure event tracing for Cisco Express Forwarding IPv4 events, use the **monitor event-trace cef ipv4** command in global configuration mode. To disable event tracing for Cisco Express Forwarding IPv4 events, use the **no** form of this command.

```
monitor event-trace cef ipv4 { disable | distribution | dump-file dump-file-name | enable | match
{ global | ip-address mask } | size number | stacktrace [depth] | vrf vrf-name [distribution |
match { global | ip-address mask } ] }
```

```
no monitor event-trace cef { ipv4 { disable | distribution | dump-file dump-file-name | enable |
match | size | stacktrace [depth] } | vrf }
```

Syntax Description		
disable		Turns off event tracing for Cisco Express Forwarding IPv4 events.
distribution		Logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards.
dump-file <i>dump-file-name</i>		Specifies the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
enable		Turns on event tracing for Cisco Express Forwarding IPv4 events if it had been enabled with the monitor event-trace cef command.
match		Turns on event tracing for Cisco Express Forwarding IPv4 that matches global events or events that match a specific network address.
global		Specifies global events.
<i>ip-address mask</i>		Specifies an IP address in A.B.C.D format and a subnet mask in A.B.C.D format.
size <i>number</i>		Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536.
	Note	Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the show monitor event-trace cef parameters command.
		When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace		Enables the stack trace at tracepoints.
<i>depth</i>		(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.
vrf <i>vrf-name</i>		Turns on event tracing for a Cisco Express Forwarding IPv4 Virtual Private Network (VPN) routing and forwarding (VRF) table. The <i>vrf-name</i> argument specifies the name of the VRF.

Command Default Event tracing for Cisco Express Forwarding IPv4 events is enabled by default.

Command Modes Global configuration (config)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **monitor event-trace cef ipv4** command to enable or disable event tracing for Cisco Express Forwarding IPv4 events.

The Cisco IOS software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef ipv4** command in privileged EXEC mode or using the **monitor event-trace cef ipv4** command in global configuration mode.

**Note**

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef ipv4** command for each instance of a trace.

To determine whether event tracing is enabled by default for Cisco Express Forwarding, use the **show monitor event-trace cef ipv4** command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for Cisco Express Forwarding IPv4 events and configure the buffer size to 5000 messages:

```
Router(config)# monitor event-trace cef ipv4 enable
```

```
Router(config)# monitor event-trace cef ipv4 size 5000
```

The following example shows how to enable event tracing for events that match Cisco Express Forwarding IPv4 VRF vpn1:

```
Router(config)# monitor event-trace cef ipv4 enable
```

```
Router(config)# monitor event-trace cef ipv4 vrf vpn1
```

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 trace-event 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.
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.

monitor event-trace cef ipv6 (global)

To configure event tracing for Cisco Express Forwarding IPv6 events, use the **monitor event-trace cef ipv6** command in global configuration mode. To disable event tracing for Cisco Express Forwarding, use the **no** form of this command.

monitor event-trace cef ipv6 { **disable** | **distribution** | **dump-file** *dump-file-name* | **enable** | **match** { **global** | *ipv6-address/n* } | **size** *number* | **stacktrace** [*depth*] | **vrf** *vrf-name* [**distribution** | **match** { **global** | *ipv6-address/n* }] }

no monitor event-trace cef ipv6 { **disable** | **distribution** | **dump-file** *dump-file-name* | **enable** | **match** | **size** | **stacktrace** [*depth*] | **vrf** }

Syntax Description		
disable		Turns off event tracing for Cisco Express Forwarding IPv6 events.
distribution		Logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards.
dump-file <i>dump-file-name</i>		Specifies the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
enable		Turns on event tracing for Cisco Express Forwarding IPv6 events if it had been enabled with the monitor event-trace cef ipv6 command.
match		Turns on event tracing for Cisco Express Forwarding IPv6 that matches global events or events that match a specific network address.
global		Specifies global events.
<i>ipv6-address/n</i>		Specifies an IPv6 address. This address must be in the form documented in RFC 2373: the address is specified in hexadecimals using 16-bit values between colons. The slash followed by a number (<i>/n</i>) indicates the number of bits that do not change. Range: 0 to 128.
size <i>number</i>		Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536.
	Note	Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the show monitor event-trace cef parameters command.
		When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace		Enables the stack trace at tracepoints.
<i>depth</i>		(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.
vrf <i>vrf-name</i>		Turns on event tracing for a Cisco Express Forwarding IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) table. The <i>vrf-name</i> argument specifies the name of the VRF.

Command Default Event tracing for Cisco Express Forwarding IPv6 events is enabled by default.

Command Modes

Global configuration (config)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **monitor event-trace cef ipv6** command to enable or disable event tracing for Cisco Express Forwarding IPv6 events.

The Cisco IOS software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef ipv6** command in privileged EXEC mode or using the **monitor event-trace cef ipv6** command in global configuration mode.

**Note**

The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef ipv6** command for each instance of a trace.

To determine whether event tracing is enabled by default for Cisco Express Forwarding IPv6 events, use the **show monitor event-trace cef ipv6** command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for Cisco Express Forwarding IPv6 events and configure the buffer size to 10000 messages.

```
Router(config)# monitor event-trace cef ipv6 enable
```

```
Router(config)# monitor event-trace cef ipv6 size 10000
```

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.
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 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 adjacency

To display information about the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table, use the **show adjacency** command in user EXEC or privileged EXEC mode.

```
show adjacency [ip-address] [interface-type interface-number | null number | port-channel
number | sysclock number | vlan number | ipv6-address | fcpa number | serial number]
[connectionid number] [link {ipv4 | ipv6 | mpls}] [detail | encapsulation]
```

```
show adjacency summary [interface-type interface-number]
```

Syntax Description

<i>ip-address</i>	(Optional) An IP address or IPv6 address. Note On the Cisco 10000 series routers IPv6 is supported on Cisco IOS Release 12.2(28)SB or later releases.
<i>interface-type</i> <i>interface-number</i>	(Optional) Interface type and number. Valid values for the <i>interface-type</i> argument are atm , async , auto-template , ctunnel , dialer , esconphy , fastethernet , filter , filtergroup , gigabitethernet , group-async , longreachethernet , loopback , mfr , multilink , portgroup , pos , tunnel , vif , virtual-template , voabypassin , voabypassout , voafilterin , voafilterout , voain , and voaout . Note Not all interface types and numbers are available on all platforms. Enter the show adjacency command to verify the interface types for your platform.
null <i>number</i>	(Optional) Specifies the null interface. The valid value is 0 .
port-channel <i>number</i>	(Optional) Specifies the channel interface; valid values are 1 to 282.
sysclock <i>number</i>	(Optional) Telecom-bus clock controller; valid values are 1 to 6.
vlan <i>number</i>	(Optional) Specifies the VLAN; valid values are 1 to 4094.
<i>ipv6-address</i>	(Optional) Specifies the associated IPv6 address.
fcpa <i>number</i>	(Optional) The fiber channel; valid values are 1 to 6.
serial <i>number</i>	(Optional) Specifies the serial interface number; valid values are 1 to 6.
connectionid <i>number</i>	(Optional) Specifies the client connection identification number.
link { ipv4 ipv6 mpls }	(Optional) Specifies the link type (IP, IPv6, or Multiprotocol Label Switching (MPLS) traffic of the adjacency).
detail	(Optional) Displays the protocol detail and timer information.
summary	(Optional) Displays a summary of Cisco Express Forwarding adjacency information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2GS	This command was introduced.
11.1CC	Multiple platform support was added.
12.0(7)XE	Support was added for the Cisco 7600 series routers.
12.1(5c)EX	This command was modified to include Layer 3 information.
12.1(11b)E	The atm , ge-wan , and pos keywords were added.
12.2(8)T	The detail keyword output was modified to show the epoch value for each entry of the adjacency table. The summary keyword output was modified to show the table epoch for the adjacency table.
12.2(14)SX	Support for this command was added for 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(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. The link ipv4 , link ipv6 , and link mpls keywords and the <i>prefix</i> argument were added.
12.2(28)SB	Support for IPv6 was added for 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.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show adjacency** command is used to verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.

For line cards, you must specify the line card if_number (interface number). Use the **show cef interface** command to obtain line card if_numbers.

You can use any combination of the *ip-address*, *interface-type*, and other keywords and arguments (in any order) as a filter to display a specific subset of adjacencies.

On Cisco 7600 series routers, hardware Layer 3-switching adjacency statistics are updated every 60 seconds.



Note

On the Cisco 10000 series routers, Pv6 is supported on Cisco IOS Release 12.2(28)SB or later releases.

The following information may be displayed by the **show adjacency** commands:

- Protocol
- Interface
- Type of routing protocol that is configured on the interface
- Type of routed protocol traffic using this adjacency
- Next hop address
- Method of adjacency that was learned
- Adjacency source (for example, Address Resolution Protocol (ARP) or ATM Map)

- Encapsulation prepended to packet switched through this adjacency
- Chain of output chain elements applied to packets after an adjacency
- Packet and byte counts
- High availability (HA) epoch and summary event epoch
- MAC address of the adjacent router
- Time left before the adjacency rolls out of the adjacency table. After the adjacency rolls out, a packet must use the same next hop to the destination.

Examples

The following examples show how to display adjacency information:

Cisco 7500 Series Router

Router# **show adjacency**

Protocol	Interface	Address
IP	FastEthernet2/3	172.20.52.1 (3045)
IP	FastEthernet2/3	172.20.52.22 (11)

The following example shows how to display adjacency information for a specific interface:

Router# **show adjacency fastethernet 0/0**

Protocol	Interface	Address
IP	FastEthernet0/0	10.4.9.2 (5)
IP	FastEthernet0/0	10.4.9.3 (5)

Cisco 10000 Series Router

Router# **show adjacency**

Protocol	Interface	Address
IP	FastEthernet2/0/0	172.20.52.1 (3045)
IP	FastEthernet2/0/0	172.20.52.22 (11)

Cisco 7500 and 10000 Series Router

The following example shows how to display detailed adjacency information for adjacent IPv6 routers:

Router# **show adjacency detail**

Protocol	Interface	Address
IP	Tunnel0	point2point(6) 0 packets, 0 bytes 00000000 CEF expires: 00:02:57 refresh: 00:00:57 Epoch: 0
IPV6	Tunnel0	point2point(6) 0 packets, 0 bytes 00000000 IPv6 CEF never Epoch: 0
IPV6	Ethernet2/0	FE80::A8BB:CCFF:FE01:9002(3) 0 packets, 0 bytes AABBCC019002AABBCC012C0286DD IPv6 ND never Epoch: 0
IPV6	Ethernet2/0	3FFE:2002::A8BB:CCFF:FE01:9002(5) 0 packets, 0 bytes

```

AABBCC019002AABBCC012C0286DD
IPv6 ND      never
Epoch: 0

```

Table 3 describes the significant fields shown in the displays.

Table 3 *show adjacency Field Descriptions*

Field	Description
Protocol	Type of Internet protocol.
Interface	Outgoing interface.
Address	Next hop IP address.

The following example shows how to display a summary of adjacency information:

```
Router# show adjacency summary
```

```

Adjacency table has 7 adjacencies:
  each adjacency consumes 368 bytes (4 bytes platform extension)
  6 complete adjacencies
  1 incomplete adjacency
  4 adjacencies of linktype IP
    4 complete adjacencies of linktype IP
    0 incomplete adjacencies of linktype IP
    0 adjacencies with fixups of linktype IP
    2 adjacencies with IP redirect of linktype IP
  3 adjacencies of linktype IPV6
    2 complete adjacencies of linktype IPV6
    1 incomplete adjacency of linktype IPV6

```

```

Adjacency database high availability:
  Database epoch: 8 (7 entries at this epoch)

```

```

Adjacency manager summary event processing:
  Summary events epoch is 52
  Summary events queue contains 0 events (high water mark 113 events)
  Summary events queue can contain 49151 events
  Adj last sourced field refreshed every 16384 summary events
  RP adjacency component enabled

```

The following examples show how to display protocol detail and timer information:

For a Cisco 7500 Series Router

```
Router# show adjacency detail
```

```

Protocol Interface      Address
IP         FastEthernet0/0 10.4.9.2(5)
                                0 packets, 0 bytes
                                epoch 0
                                sourced in sev-epoch 2
                                Encap length 14
                                00307131ABFC000500509C080800
                                ARP
IP         FastEthernet0/0 10.4.9.3(5)
                                0 packets, 0 bytes
                                epoch 0
                                sourced in sev-epoch 2
                                Encap length 14

```

```
000500506C08000500509C080800
ARP
```

For a Cisco 7600 Series Router

```
Router# show adjacency detail
```

```
Protocol Interface Address
IP         FastEthernet2/3 172.20.52.1(3045)
0 packets, 0 bytes
000000000FF920000380000000000000
00000000000000000000000000000000
00605C865B2800D0BB0F980B0800
ARP        03:58:12
IP         FastEthernet2/3 172.20.52.22(11)
0 packets, 0 bytes
000000000FF920000380000000000000
00000000000000000000000000000000
00801C93804000D0BB0F980B0800
ARP        03:58:06
```

For a Cisco 10000 Series Router

```
Router# show adjacency detail
```

```
Protocol Interface Address
IP         FastEthernet2/0/0 10.4.9.2(5)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 2
Encap length 14
00307131ABFC000500509C080800
ARP
IP         FastEthernet2/0/0 10.4.9.3(5)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 2
Encap length 14
000500506C08000500509C080800
ARP
```

The following examples show how to display protocol detail and timer adjacency information for IP links for a specific interface:

For a Cisco 7500 Series Router

```
Router# show adjacency tunnel 1 link detail
```

```
Protocol Interface Address
IP         Tunnel1      point2point(7)
0 packets, 0 bytes
epoch 1
sourced in sev-epoch 4
empty encap string
P2P-ADJ
Next chain element:
label 16 TAG adj out of Ethernet1/0, addr 10.0.0.0
```

For a Cisco 7600 Series Router

Router# **show adjacency fastethernet 2/3**

Protocol	Interface	Address
IP	FastEthernet2/3	172.20.52.1(3045)
IP	FastEthernet2/3	172.20.52.22(11)

For a Cisco 10000 Series Router

Router# **show adjacency tunnel 1 link detail**

Protocol	Interface	Address
IP	Tunnell	point2point(7) 0 packets, 0 bytes epoch 1 sourced in sev-epoch 4 empty encap string P2P-ADJ Next chain element: label 16 TAG adj out of FastEthernet0/0, addr 10.0.0.0

Related Commands

Command	Description
clear adjacency	Clears the Cisco Express Forwarding adjacency table.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show adjacency	Enables the display of information about the adjacency database.
show mls cef adjacency	Displays information about the hardware Layer 3-switching adjacency node.
show cef interface	Displays detailed Cisco Express Forwarding information for all interfaces.

show cef

To display information about packets forwarded by Cisco Express Forwarding, use the **show cef** command in privileged EXEC mode.

```
show cef {accounting | background [detail] | broker broker-name [detail] | error | fib |
hardware vectors | idb | loadinfo | non-ip | nsf | path [list [walk] | sets [detail | id path-set-id
| summary] | switching background [detail] | walks [process | queue]}
```

Syntax Description		
accounting		Displays Cisco Express Forwarding accounting state.
background		Displays Cisco Express Forwarding background processing.
detail		(Optional) Displays detailed Cisco Express Forwarding information.
broker <i>broker-name</i>		(Distributed platforms only) Displays Cisco Express Forwarding information related to update brokers.
error		Displays information about the state of Cisco Express Forwarding errors.
fib		Displays Cisco Express Forwarding Forwarding Information Base (FIB) entries.
hardware vectors		Displays the hardware application programming interface (API) vector function table.
idb		Displays Cisco Express Forwarding interface descriptor blocks.
loadinfo		Displays Cisco Express Forwarding loadinfo events.
non-ip		Displays Cisco Express Forwarding paths for non-IP traffic.
nsf		(Distributed platforms only) Displays Cisco Express Forwarding nonstop forwarding (NSF) statistics.
path		Displays Cisco Express Forwarding paths.
list		(Optional) Displays a list of Cisco Express Forwarding paths.
walk		(Optional) Displays the walk through the list of Cisco Express Forwarding paths.
sets		(Optional) Displays point-to-multipoint path set information.
detail		(Optional) Displays detailed point-to-multipoint path set information.
id <i>path-set-id</i>		(Optional) Displays information about the specified path set. Enter the path set ID in hex format.
summary		(Optional) Displays high-level information about point-to-multipoint path sets.
switching background		Display Cisco Express Forwarding background switching processing.
walks		Specifies a walk through Cisco Express Forwarding infrastructure.
process		(Optional) Displays the process that services the background work queue.
queue		(Optional) Displays the work queue of background walks.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2GS	This command was introduced to support the Cisco 12012 Internet router.
11.1CC	Support was added for multiple platforms.
12.0(22)S	The display output for this command was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 packets.
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(25)S	The drop and not-cef-switched keywords were removed. The accounting , background , broker , fib , hardware vectors , idb , loadinfo , non-ip , nsf , path , and walks keywords were added.
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.
12.2(33)SRE	This command was modified. The sets keyword was added to display point-to-multipoint information.

Usage Guidelines

Use this command to display and monitor information about traffic forwarded by Cisco Express Forwarding.

A line card might drop packets because of encapsulation failure, absence of route information, or absence of adjacency information.

A packet is punted (sent to another switch path) because Cisco Express Forwarding may not support a specified encapsulation or feature, the packet may be destined for the router, or the packet may have IP options (such as time stamp and record route). IP options are process switched.

Examples

The following example shows how to display Cisco Express Forwarding accounting information:

```
Router# show cef accounting
```

```
IPv4 accounting state:
```

```
  Enabled accounting:      per-prefix, non-recursive, prefix-length
  Non-recursive load interval: 30 (default 30)
  Non-recursive update interval: 0 (default 0)
```

```
IPv6 accounting state:
```

```
  Enabled accounting:      None
  Non-recursive load interval: 30 (default 30)
  Non-recursive update interval: 0 (default 0)
```

[Table 4](#) describes the significant fields shown in the example.

Table 4 *show cef accounting Field Descriptions*

Field	Description
Enabled accounting	Type or types of Cisco Express Forwarding accounting that are enabled: load-balance-hash, non-recursive, per-prefix, prefix-length, or none.
per-prefix	Indicates that Cisco Express Forwarding accounting is enabled for the collection of the number of packets and bytes express-forwarded to a destination (or prefix).
non-recursive	Indicates that Cisco Express Forwarding accounting is enabled through nonrecursive prefixes.
prefix-length	Indicates that Cisco Express Forwarding accounting is enabled through prefix length.

The following example shows how to display Cisco Express Forwarding background information:

```
Router# show cef background
```

```
CEF background process process (pid 77) running
 0 events awaiting registration on background process
 9 events registered on background process
  boolean   FIB malloc failed, 0 occurrences
  boolean   FIB assert failed, 0 occurrences
  boolean   FIB hw_api_failure failed, 0 occurrences
  timer     FIB checkers: auto-repair delay, init, !run, 0 occurrences
  timer     FIB checkers: auto-repair delay, init, !run, 0 occurrences
  timer     FIB checkers: IPv4 scan-rib-ios scanner, init, run, 2 occurrences
  timer     FIB checkers: IPv4 scan-ios-rib scanner, init, run, 2 occurrences
  timer     FIB checkers: IPv6 scan-ios-rib scanner, init, run, 2 occurrences
  timer     FIB table: rate monitor, init, run, 0 occurrences
```

Table 5 describes the significant fields shown in the example.

Table 5 *show cef background Field Descriptions*

Field	Description
boolean	The background process is waiting for a true or false flag to be set.
FIB malloc failed, 0 occurrences	No instances of memory allocation failure have occurred for the FIB.
FIB assert failed, 0 occurrences	No instances of assertion failure have occurred for the FIB.
FIB hw_api_failure failed; 0 occurrences	No failures are reported during the programming of hardware forwarding.
timer	The background process is waiting for a timer to be triggered. Once the timer is triggered, the operation begins. In the FIB checkers cases that follow, the timer is linked to Cisco Express Forwarding consistency checkers.
FIB checkers: auto-repair delay, init, !run, 0 occurrences	FIB auto repair timer is initialized, but the timer is not running and has not been running (0 occurrences).
FIB checkers: IPv4 scan-rib-ios scanner, init, !run, 2 occurrences	FIB IPv4 scan-rib-ios timer is initialized and running. The timer has been triggered twice.

Table 5 *show cef background Field Descriptions*

Field	Description
FIB checkers: IPv4 scan-ios-rib scanner, init, run, 2 occurrences	FIB IPv4 scan-ios-rib timer is initialized and running. The timer has been triggered twice.
FIB table: rate monitor, init, run, 0 occurrences	FIB table rate monitor timer is initialized and running, but has yet to be triggered.

The following example shows how to display information about Cisco Express Forwarding FIB entries:

```
Router# show cef fib
```

```
9 allocated IPv4 entries, 0 failed allocations
1 allocated IPv6 entry, 0 failed allocations
```

Table 6 describes the significant fields shown in the example.

Table 6 *show cef fib Field Descriptions*

Field	Description
9 allocated IPv4 entries, 0 failed allocations	Number of successfully allocated and failed IPv4 entries.
1 allocated IPv6 entry, 0 failed allocations	Number of successfully allocated and failed IPv6 entries.

The following example shows how to display information about Cisco Express Forwarding loadinfo:

```
Router# show cef loadinfo
```

```
0 allocated loadinfos, 0 failed allocations
0 allocated loadinfo hash usage gsbs
0 inplace modifies (enabled)
0 identical modifies
```

Table 7 describes the significant fields shown in the example.

Table 7 *show cef loadinfo Field Descriptions*

Field	Description
0 allocated loadinfos, 0 failed allocations	Number of successfully allocated and failed allocated loadinfos.
0 allocated loadinfo hash usage gsbs	Number of allocated subblocks for per-hash bucket accounting when load balancing is used.
0 inplace modifies (enabled)	In-place modification is enabled. No in-place modifications have occurred.
0 identical modifies	Number of in-place modifications that were skipped because the replacement was identical to the target.

The following example shows how to display information for Cisco Express Forwarding paths:

```
Router# show cef path
```

```
28 allocated IPv4 paths, 0 failed allocations
4 allocated IPv6 paths, 0 failed allocations
```


32 Total Paths, 587 Recursive Paths, 0 Unresolved Paths

Table 8 describes the significant fields shown in the example.

Table 8 *show cef path Field Descriptions*

Field	Definition
28 allocated IPv4 paths	Number of successfully allocated and failed IPv4 paths.
4 allocated IPv6 paths	Number of successfully allocated and failed IPv6 paths.
32 Total Paths, 587 Recursive Paths, 0 Unresolved Paths	Information on all Cisco Express Forwarding paths.

The following example shows how to display information about Cisco Express Forwarding background switching processes:

```
Router# show cef switching background
```

```
CEF switching background process (pid 46) running
 0 events awaiting registration on background process
 1 event registered on background process
 boolean   OCE unlock queue, 0 occurrences
```

Table 9 describes the significant fields shown in the example.

Table 9 *show cef switching background Field Descriptions*

Field	Description
0 events awaiting registration on background process	Number of events waiting to be registered on the background process.
1 event registered on background process	Number of events registered on the background process.
boolean OCE unlock queue, 0 occurrences	Number of output chain element (OCE) unlock queue events.

The following example shows how to display information about Cisco Express Forwarding:

```
Router# show cef walks
```

```
Calling process:
```

```
-----
```

```
Number of initial walks:
```

```

                                started
mode / priority      low      high      very high
sync                 3         0         0
atomic               0         0         0

                                finished
mode / priority      low      high      very high
sync                 3         0         0
atomic               0         0         0

                                restarted
mode / priority      low      high      very high
```

```

sync                0                0                0
atomic              0                0                0

Number of sub walks:

mode / priority      started
                    low          high      very high
sync                0                0                0
atomic              0                0                0

mode / priority      finished
                    low          high      very high
sync                0                0                0
atomic              0                0                0

```

Table 10 describes the significant fields shown in the example.

Table 10 *show cef walks Field Description*

Field	Description
mode	Indicates the mode of the Cisco Express Forwarding infrastructure walk: - sync—The walk takes place in the current process context and completes before the start function returns. Other processes are allowed to run. - atomic—The walk takes place in the current process context and completes before the start function returns. No other processes are allowed to run.
priority	Indicate the priority of the infrastructure walk: low, medium, or high.

Related Commands

Command	Description
clear cef linecard	Clears Cisco Express Forwarding information from line cards.
show cef features global	Displays Cisco Express Forwarding features for any interface.
show cef interface	Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces.
show cef linecard	Displays Cisco Express Forwarding-related information by line card.
show cef memory	Displays information about Cisco Express Forwarding memory usage.
show cef state	Displays the state of Cisco Express Forwarding on a networking device.
show cef subtree context client	Displays Cisco Express Forwarding prefix subtrees.
show cef table	Displays the configuration and operational state of the Cisco Express Forwarding FIB table.
show cef timers	Displays the current state of the timers internal to the Cisco Express Forwarding process.

show cef drop



Note

The **show cef drop** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases.

To display a list of which packets each line card dropped, use the **show cef drop** command in user EXEC or privileged EXEC mode.

show cef drop

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.
12.0(22)S	The display output for this command was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 packets.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. Previously there was a show cef command, and drop was a keyword of that command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2S releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Usage Guidelines

A line card might drop packets because of encapsulation failure, absence of route information, or absence of adjacency information.

A packet is sent to a different switching path (punted) because Cisco Express Forwarding does not support the encapsulation or feature, the packet is destined for the router, or the packet has IP options, such as time stamp and record route. IP options are process switched.

**Note**

If Cisco Express Forwarding for IPv6 or distributed Cisco Express Forwarding for IPv6 is enabled globally on the router, the **show cef drop** command displays IPv6 Cisco Express Forwarding counter information and IPv4 Cisco Express Forwarding counter information. If Cisco Express Forwarding for IPv6 or distributed Cisco Express Forwarding for IPv6 is not enabled globally on the router, the command displays only IPv4 Cisco Express Forwarding counter information.

Examples

The following is sample output from the **show cef drop** command:

```
Router# show cef drop
```

```
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChksumErr
RP           4           89           0           4           0           0
1           0           0           0           0           0           0
2           0           0           5           0           0           5

IPv6 CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj
RP           2           33           0           2           0
1           0           0           3           0           0
2           0           0           0           0           0
```

Table 11 describes the significant fields shown in the display.

Table 11 *show cef drop Field Descriptions*

Field	Description
Slot	The slot number on which the packets were received.
Encap_fail	Indicates the number of packets dropped after exceeding the limit for packets punted to the processor due to missing adjacency information (Cisco Express Forwarding throttles packets passed up to the process level at a rate of one packet every two seconds).
Unresolved	Indicates the number of packets dropped due to an unresolved prefix in the Forwarding Information Base (FIB) table.
Unsupported	Indicates the number of packets fast-dropped by Cisco Express Forwarding (drop adjacency).
No_route	Indicates the number of packets dropped due to a missing prefix in the FIB table.
No_adj	Indicates the number of packets dropped due to incomplete adjacency.
ChksumErr	Indicates the number of IPv4 packets received with a checksum error. Note This field is not supported for IPv6 packets.

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.

show cef events



Note

The **show cef events** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases.

To display a list of events internal to the Cisco Express Forwarding process, use the **show cef events** command in user EXEC or privileged EXEC mode.

show cef events

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2S releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Examples

The following is sample output from the **show cef events** command:

```
Router# show cef events
```

```
CEF events (14/0 recorded/ignored)
```

Time	Event	Details
+00:00:00.000	SubSys	ipfib init
+00:00:00.000	SubSys	ipfib_ios init
+00:00:00.000	SubSys	ipfib_util init
+00:00:00.000	SubSys	adj_ios init
+00:00:00.000	SubSys	ipfib_les init
+00:00:01.272	Flag	FIB enabled set to yes
+00:00:01.272	Flag	FIB switching enabled set to yes
+00:00:01.272	GState	CEF enabled
+00:00:02.872	Process	Background created

```

+00:00:02.872  Flag      FIB running set to yes
+00:00:02.872  Process   Background event loop enter
+00:00:02.912  Flag      FIB switching running set to yes
+00:00:02.920  Process   Scanner created
+00:00:02.920  Process   Scanner event loop enter

```

Table 12 describes the significant fields shown in the display.

Table 12 *show cef events Field Descriptions*

Field	Description
Time	Time that the event occurred.
Event	Type of event that occurred.
Details	Detailed description of the event.

Related Commands

Command	Description
show cef drop	Displays a list of which packets each line card dropped.
show cef interface	Displays Cisco Express Forwarding-related interface information.
show cef linecard	Displays Cisco Express Forwarding-related interface information by line card.

show cef features global

To display Cisco Express Forwarding features for any interface, use the **show cef features global** command in privileged EXEC mode.

show cef features global

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	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 This command is used to determine if Cisco Express Forwarding is enabled for all interfaces.

Examples The following is sample output from the **show cef features global** command:

```
Router# show cef features global
```

```
Global Drop features not attached to a specific interface:
  Input FNF
Global Punt features not attached to a specific interface:
  Input FNF, SPD Classify
```

[Table 13](#) describes the significant fields shown in the display.

Table 13 *show cef features global Field Descriptions*

Field	Description
Input FNF	Flexible NetFlow (FNF) feature.
SPD Classify	Flexible NetFlow (FNF) feature.

This output shows the global drop feature, Flexible NetFlow (Input FNF), and two global punt features, Input FNF and SPD Classify. SPD Classify is present by default. The punt features are invoked for all punted packets regardless of the interface upon which they are received.

Related Commands	Command	Description
	show cef interface	Displays detailed Cisco Express Forwarding information for all interfaces.

show cef interface

To display detailed Cisco Express Forwarding information for a specified interface or for all interfaces, use the **show cef interface** command in user EXEC or privileged EXEC mode.

show cef interface [*type number*] [**statistics** | **detail** | **internal** | **brief** | **policy-statistics** [**input** | **output**]]

Syntax Description	
<i>type number</i>	(Optional) Interface type and number. No space is required between the interface type and number.
statistics	(Optional) Displays switching statistics for an interface or interfaces.
detail	(Optional) Displays detailed Cisco Express Forwarding information for the specified interface type and number.
internal	(Optional) Displays internal Cisco Express Forwarding interface status and configuration.
brief	(Optional) Summarizes the Cisco Express Forwarding interface state.
policy-statistics	(Optional) Displays Border Gateway Protocol (BGP) policy statistical information for a specific interface or for all interfaces.
input	(Optional) Displays BGP accounting policy statistics for traffic that is traveling through an input interface.
output	(Optional) Displays BGP accounting policy statistics for traffic that is traveling through an output interface.

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

Command History	Release	Modification
	11.2GS	This command was introduced to support the Cisco 12012 Internet router.
	11.1CC	Support for multiple platforms was added.
	12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST, and the statistics keyword was added.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T, and the detail keyword was added.
	12.2(13)T	The policy-statistics keyword was added.
	12.0(22)S	The input and output keywords were added. The display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding interface information. Output fields that support BGP policy accounting were added for the Cisco 7200 series and Cisco 7500 series platforms.

Release	Modification
12.3(4)T	The input and output keywords were added. The display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding interface information. Output fields that support BGP policy accounting were added for the Cisco 7200 series and Cisco 7500 series platforms.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The internal keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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

You can use this command to display the detailed Cisco Express Forwarding status for all interfaces.

Values entered for the *type* and *number* arguments display Cisco Express Forwarding status information for the specified interface type and number.

The **policy-statistics**, **input**, and **output** keywords are available only on distributed switching platforms.

Examples

The following example shows how to display a summary of Cisco Express Forwarding information for an interface named Ethernet 3/0:

```
Router# show cef interface ethernet 3/0 brief
```

```
Interface                IP-Address      Status  Switching
Ethernet3/0              10.0.212.6      up      CEF
Router#
```

The following is sample output from the **show cef interface** command for Fast Ethernet interface 1/0/0 with BGP policy accounting configured for input traffic:

```
Router# show cef interface fastethernet 1/0/0
```

```
FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  Internet address is 10.1.1.1/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is enabled
  BGP based policy accounting on output is disabled
Hardware idb is FastEthernet1/0/0 (6)
Software idb is FastEthernet1/0/0 (6)
Fast switching type 1, interface type 18
IP Distributed CEF switching enabled
IP Feature Fast switching turbo vector
IP Feature CEF switching turbo vector
Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
```

```

ifindex 7(7)
Slot 1 Slot unit 0 VC -1
Transmit limit accumulator 0xE8001A82 (0xE8001A82)
IP MTU 1500

```

The following is sample output from the **show cef interface detail** command for Ethernet interface 1/0/0:

Router# **show cef interface ethernet 1/0/0 detail**

```

FastEthernet1/0/0 is up (if_number 6)
  Corresponding hwidb fast_if_number 6
  Corresponding hwidb firstsw->if_number 6
  Internet address is 10.1.1.1/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is enabled
  BGP based policy accounting on output is disabled
  Hardware idb is FastEthernet1/0/0 (6)
  Software idb is FastEthernet1/0/0 (6)
  Fast switching type 1, interface type 18
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0xE8001A82 (0xE8001A82)
  IP MTU 1500

```

The following is sample output from the **show cef interface Null 0 detail** command:

Router# **show cef interface null 0 detail**

```

Null0 is up (if_number 1)
  Corresponding hwidb fast_if_number 1
  Corresponding hwidb firstsw->if_number 1
  Internet Protocol processing disabled
  Interface is marked as nullidb
  Packets switched to this interface on linecard are dropped to next slow path
  Hardware idb is Null0
  Fast switching type 13, interface type 0
  IP CEF switching enabled
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 0(0)
  Slot -1 Slot unit -1 VC -1
  Transmit limit accumulator 0x0 (0x0)
  IP MTU 1500

```

The following is sample output for internal Cisco Express Forwarding interface status and configuration for the Ethernet 3/1 interface:

Router# **show cef interface ethernet 3/1 internal**

```

Ethernet3/1 is up (if_number 13)
  Corresponding hwidb fast_if_number 13
  Corresponding hwidb firstsw->if_number 13
  Internet address is 10.0.212.6/24
  ICMP redirects are always sent

```

```

Per packet load-sharing is disabled
IP unicast RPF check is disabled
Inbound access list is not set
Outbound access list is not set
IP policy routing is disabled
BGP based policy accounting on input is disabled
BGP based policy accounting on output is disabled
Hardware idb is Ethernet3/1
Fast switching type 1, interface type 63
IP CEF switching enabled
IP CEF switching turbo vector
IP CEF turbo switching turbo vector
IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
Input fast flags 0x0, Output fast flags 0x0
ifindex 11(11)
Slot 3 Slot unit 0 VC -1
Transmit limit accumulator 0x0 (0x0)
IP MTU 1500
Subblocks:
  IPv6: enabled 1 unreachable FALSE redirect TRUE mtu 1500 flags 0x0
        link-local address is FE80::20C:CFFF:FEF9:4854
        Global unicast address(es):
          10:6:6:6:20C:CFFF:FEF9:4854, subnet is 10:6:6:6::/64 [EUI]
  IPv4: Internet address is 10.0.212.6/24
        Broadcast address 255.255.255.255
        Per packet load-sharing is disabled
        IP MTU 1500

```

Table 14 describes the significant fields shown in the displays.

Table 14 *show cef interface Field Descriptions*

Field	Description
FastEthernet1/0/0 is up	Indicates type, number, and status of the interface.
Internet address is	Internet address of the interface.
ICMP redirects are always sent	Indicates how packet forwarding is configured.
Per packet load-sharing is disabled	Indicates status of load sharing on the interface.
IP unicast RPF check is disabled	Indicates status of IP unicast Reverse Path Forwarding (RPF) check on the interface.
Inbound access list is not set	Indicates the number or name of the inbound access list if one is applied to this interface. Also indicates whether the list is set.
Outbound access list is not set	Indicates the number or name of the outbound access list if one is applied to this interface. Also indicates whether the list is set.
IP policy routing is disabled	Indicates the status of IP policy routing on the interface.
BGP based policy accounting on input is enabled	Indicates the status of BGP policy accounting on the input interface.
BGP based policy accounting on output is disabled	Indicates the status of BGP policy accounting on the output interface.
Hardware idb is Ethernet1/0/0	Interface type and number configured.

Table 14 *show cef interface Field Descriptions (continued)*

Field	Description
Fast switching type	Used for troubleshooting; indicates switching mode in use.
Interface type	Indicates interface type.
IP Distributed CEF switching enabled	Indicates whether distributed Cisco Express Forwarding is enabled on this interface. (Cisco 7500 and 12000 series Internet routers only.)
IP Feature Fast switching turbo vector	Indicates IP fast switching type configured.
IP Feature CEF switching turbo vector	Indicates IP feature Cisco Express Forwarding switching type configured.
Input fast flags	Indicates the input status of various switching features: • 0x0001 (input Access Control List [ACL] enabled) • 0x0002 (policy routing enabled) • 0x0004 (input rate limiting) • 0x0008 (MAC/Prec accounting) • 0x0010 (DSCP/PREC/QOS GROUP) • 0x0020 (input named access lists) • 0x0040 (NAT enabled on input) • 0x0080 (crypto map on input) • 0x0100 (QPPB classification) • 0x0200 (inspect on input) • 0x0400 (input classification) • 0x0800 (¹casa input enable) • 0x1000 (Virtual Private Network [VPN] enabled on a ²swidb) • 0x2000 (input idle timer enabled) • 0x4000 (unicast Reverse Path Forwarding [RPF] check) • 0x8000 (per-address ACL enabled) • 0x10000 (deaggregating a packet) • 0x20000 (³GPRS enabled on input) • 0x40000 (URL RenDezvous) • 0x80000 (QoS classification) • 0x100000 (FR switching on interface) • 0x200000 (⁴WCCP redirect on input) • 0x400000 (input classification)

Table 14 *show cef interface Field Descriptions (continued)*

Field	Description
Output fast flags	Indicates the output status of various switching features, as follows: • 0x0001 (output ACL enabled) • 0x0002 (IP accounting enabled) • 0x0004 (WCC redirect enabled interface) • 0x0008 (rate limiting) • 0x0010 (MAC/Prec accounting) • 0x0020 (DSCP/PREC/QOS GROUP) • 0x0040 (D-QOS classification) • 0x0080 (output named access lists) • 0x0100 (NAT enabled on output) • 0x0200 (TCP intercept enabled) • 0x0400 (crypto map set on output) • 0x0800 (output firewall) • 0x1000 (⁵RSVP classification) • 0x2000 (inspect on output) • 0x4000 (QoS classification) • 0x8000 (QoS preclassification) • 0x10000 (output stile)
ifindex 7/(7)	Indicates a Cisco IOS internal index or identifier for this interface.
Slot 1 Slot unit 0 VC -1	The slot number and slot unit.
Transmit limit accumulator	Indicates the maximum number of packets allowed in the transmit queue.
IP MTU	The MTU size set on the interface.

1. Cisco applications and services architecture (CASA)
2. Software interface descriptor block (SWIDB)
3. General packet radio system (GPRS)
4. Web cache communication protocol (WCCP)
5. Resource reservation protocol (RSVP)

The following is sample output from the **show cef interface command** using the **policy-statistics** keyword:

```
Router# show cef interface policy-statistics
```

```
POS7/0 is up (if_number 8)
Index   Packets          Bytes
1         0                0
2         0                0
3        50          5000
```

4	100	10000
5	100	10000
6	10	1000
7	0	0
8	0	0

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for Ethernet interface 1/0.

```
Router# show cef interface ethernet 1/0 policy-statistics
```

```
Ethernet1/0 is up (if_number 3)
Corresponding hwidb fast_if_number 3
Corresponding hwidb firstsw->if_number 3
```

Index	Packets	Bytes
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for Fast Ethernet interface 1/0/0 with the policy accounting based on input traffic.

```
Router# show cef interface fastethernet 1/0/0 policy-statistics input
```

```
FastEthernet1/0/0 is up (if_number 6)
Corresponding hwidb fast_if_number 6
Corresponding hwidb firstsw->if_number 6
BGP based Policy accounting on input is enabled
```

Index	Packets	Bytes
1	9999	999900
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0
29	0	0

30	0	0
31	0	0
32	0	0
33	0	0
34	1234	123400
35	0	0
36	0	0
37	0	0
38	0	0
39	0	0
40	0	0
41	0	0
42	0	0
43	0	0
44	0	0
45	1000	100000
46	0	0
47	0	0
48	0	0
49	0	0
50	0	0
51	0	0
52	0	0
53	0	0
54	5123	1198782

The following is sample output from the **show cef interface** command using the **policy-statistics** keyword. It shows policy statistics for serial interface 1/1/2 with the policy accounting based on output traffic.

```
Router# show cef interface serial 1/1/2 policy-statistics output
```

```
Serial1/1/2 is up (if_number 9)
Corresponding hwidb fast_if_number 9
Corresponding hwidb firstsw->if_number 9
BGP based Policy accounting on output is enabled
```

Index	Packets	Bytes
1	9999	999900
2	0	0
.		
.		
.		
18	0	0
19	0	0
20	0	0
.		
.		
.		
34	1234	123400
35	0	0
.		
.		
.		
44	0	0
45	1000	100000
46	0	0
47	0	0
48	0	0
49	0	0
50	0	0
51	0	0
52	0	0
53	0	0
54	5123	1198782

55	0	0
56	0	0
57	0	0
58	0	0
59	0	0
60	0	0
61	0	0
62	0	0
63	0	0
64	0	0

Table 15 describes the significant fields shown in the display.

Table 15 *show cef interface policy-statistics Field Descriptions*

Field	Description
Index	Traffic index set with the route-map command.
Packets	Number of packets switched that match the index definition.
Bytes	Number of bytes switched that match the index definition.

Related Commands

Command	Description
clear cef linecard	Clears Cisco Express Forwarding information from line cards.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
show cef	Displays information about packets forwarded by Cisco Express Forwarding.
show cef drop	Displays which packets the line cards dropped, or displays which packets were not express forwarded.
show cef linecard	Displays Cisco Express Forwarding interface information by line card.

show cef interface policy-statistics

To display Cisco Express Forwarding policy statistical information for a specific interface or for all interfaces, use the **show cef interface policy-statistics** command in user EXEC or privileged EXEC mode.

show cef interface [*type number*] **policy-statistics** [**input** | **output**]

Syntax Description	<i>type number</i>	(Optional) Interface type and number. A space is not required between the interface type and number.
	input	(Optional) Displays Border Gateway Protocol (BGP) policy accounting statistics for traffic that is traveling through an input interface.
	output	(Optional) Displays BGP policy accounting statistics for traffic that is traveling through an output interface.
Command Default	By default, this command displays the input statistics only.	
Command Modes	User EXEC (>) Privileged EXEC (#)	
Command History	Release	Modification
	12.0(9)S	This command was introduced on the Cisco 12000 series Internet routers.
	12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.0(22)S	The input and output keywords were added.
		The display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 interface information. Output fields that support BGP policy accounting were added for the Cisco 7200 series and Cisco 7500 series platforms.
	12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
	12.3(4)T	Changes to this command were integrated into Cisco IOS Release 12.3(4)T.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Usage Guidelines	This command is available on all software switching platforms, such as the Cisco 7200 series router, and distributed switched platforms, such as the Route Switch Processor (RSP), Gigabit Switch Router (GSR), and the Catalyst 6000 series router. This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.	

Two sets of counters are displayed for BGP policy accounting: input counters and output counters. If you enter the **show cef interface policy-statistics** command without an optional keyword, the command displays only input counters. If you want to display the output counters, you must enter the command with the **output** keyword. You can also display the input counters by entering the **input** keyword with the command.

The number of lines in the output of the **show cef interface policy-statistics** command varies from platform to platform. The software switched platforms support 64 input and 64 output counters and thus 64 lines of output. The Catalyst 6000 family switches and Cisco 7600 series routers support seven input and seven output counters and seven lines of output.

You enable BGP policy accounting on a particular interface when you enter the **bgp-policy accounting** command in interface configuration mode. To define the conditions for BGP policy accounting, you use the **set traffic-index** command in route-map configuration mode, the **route-map** command in global configuration mode, the **table-map** command in route-map configuration mode, and the **match** command in route-map configuration mode. The **table-map** command adds the named route map to the BGP routing table. BGP uses the route map name to set traffic indexes for routes in the IP routing table. The **match** commands specify the match criteria—the conditions under which policy routing occurs. The **set traffic-index** command sets the traffic indexes for matching prefixes. The **show ip cef detail** command displays the traffic index for any particular route.

Examples

The following is sample output from the **show cef interface policy-statistics** command:

```
Router# show cef interface policy-statistics
```

```
POS7/0 is up (if_number 8)
```

Index	Packets	Bytes
1	0	0
2	0	0
3	50	5000
4	100	10000
5	100	10000
6	10	1000
7	0	0
8	0	0

The following is sample output from the **show cef interface policy-statistics** command showing policy statistics for Ethernet interface 1/0:

```
Router# show cef interface ethernet 1/0 policy-statistics
```

```
Ethernet1/0 is up (if_number 3)
```

```
Corresponding hwidb fast_if_number 3
```

```
Corresponding hwidb firstsw->if_number 3
```

Index	Packets	Bytes
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0

The following is sample output from the **show cef interface policy-statistics** command showing policy statistics for Fast Ethernet interface 1/0/0 with the policy accounting based on input traffic:

```
Router# show cef interface fastethernet 1/0/0 policy-statistics input
```

FastEthernet1/0/0 is up (if_number 6)
 Corresponding hwidb fast_if_number 6
 Corresponding hwidb firstsw->if_number 6
 BGP based Policy accounting on input is enabled

Index	Packets	Bytes
1	9999	999900
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0
29	0	0
30	0	0
31	0	0
32	0	0
33	0	0
34	1234	123400
35	0	0
36	0	0
37	0	0
38	0	0
39	0	0
40	0	0
41	0	0
42	0	0
43	0	0
44	0	0
45	1000	100000
46	0	0
47	0	0
48	0	0
49	0	0
50	0	0
51	0	0
52	0	0
53	0	0
54	5123	1198782
55	0	0
56	0	0
57	0	0
58	0	0
59	0	0

60	0	0
61	0	0
62	0	0
63	0	0
64	0	0

The following is sample output from the **show cef interface policy-statistics** command showing policy statistics for serial interface 1/1/2 with the policy accounting based on output traffic:

Router# **show cef interface serial 1/1/2 policy-statistics output**

```
Serial1/1/2 is up (if_number 9)
Corresponding hwidb fast_if_number 9
Corresponding hwidb firstsw->if_number 9
BGP based Policy accounting on output is enabled
```

Index	Packets	Bytes
1	9999	999900
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0
29	0	0
30	0	0
31	0	0
32	0	0
33	0	0
34	1234	123400
35	0	0
36	0	0
37	0	0
38	0	0
39	0	0
40	0	0
41	0	0
42	0	0
43	0	0
44	0	0
45	1000	100000
46	0	0
47	0	0
48	0	0

49	0	0
50	0	0
51	0	0
52	0	0
53	0	0
54	5123	1198782
55	0	0
56	0	0
57	0	0
58	0	0
59	0	0
60	0	0
61	0	0
62	0	0
63	0	0
64	0	0

Table 16 describes the significant fields shown in these displays.

Table 16 *show cef interface policy-statistics Field Descriptions*

Field	Description
Index	Traffic index set with the route-map command.
Packets	Number of packets switched that match the index definition.
Bytes	Number of bytes switched that match the index definition.

Related Commands

Command	Description
bgp-policy	Enables BGP policy accounting or policy propagation on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match extcommunity	Matches BGP extended community list attributes.
match local-preference	Configures a route map to match routes based on the BGP local-preference attribute.
match policy-list	Configures a route map to evaluate and process a BGP policy list in a route map.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another or enables policy routing.
set traffic-index	Indicates how to classify packets that pass a match clause of a route map for BGP policy accounting.
show cef drop	Displays which packets were dropped by the line cards or displays which packets were not express forwarded.
show cef linecard	Displays Cisco Express Forwarding-related interface information by line card.
show ip cef detail	Displays a detailed summary of the FIB.
table-map	Modifies metric and tag values when the IP routing table is updated with BGP learned routes.

show cef linecard

To display Cisco Express Forwarding-related information by line card, use the **show cef linecard** command in user EXEC or privileged EXEC mode.

show cef linecard [*slot-number*] [**detail**] [**internal**]

Syntax Description	<i>slot-number</i>	(Optional) Slot number for the line card about which to display Cisco Express Forwarding-related information. When you omit this argument, information about all line cards is displayed.
	detail	(Optional) Displays detailed Cisco Express Forwarding information for the specified line card.
	internal	(Optional) Displays internal Cisco Express Forwarding information for the specified line card.

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

Command History	Release	Modification
	11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
	11.1 CC	Multiple platform support was added.
	12.0(10)S	Output display was changed.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and the display output was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 line card information.
	12.2(13)T	The display output modifications made in Cisco IOS Release 12.0(22)S were 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(25)S	The events keyword was removed.
	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 This command is available only on distributed switching platforms.

When you omit the *slot-number* argument, information about all line cards is displayed. When you omit the *slot-number* argument and include the **detail** keyword, detailed information is displayed for all line cards. When you omit the *slot-number* argument and include the **internal** keyword, detailed internal information is displayed for all line cards. When you omit all keywords and arguments, the **show cef linecard** command displays important information about all line cards in table format.

Examples

The following is sample output from the **show cef linecard** command. The command displays information for all line cards in table format.

```
Router# show cef linecard
```

Slot	MsgSent	XDRSent	Window	LowQ	MedQ	HighQ	Flags
0	6	95	24	0	0	0	up
1	6	95	24	0	0	0	up

VRF Default-table, version 8, 6 routes

Slot	Version	CEF-XDR	I/Fs	State	Flags
0	7	4	8	Active	up, sync
1	7	4	10	Active	up, sync

The following is sample output from the **show cef linecard detail** command for all line cards:

```
Router# show cef linecard detail
```

```
CEF linecard slot number 0, status up
Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
Send failed 0, Out Of Sequence 0, drops 0
Linecard CEF reset 0, reloaded 1
95 elements packed in 6 messages(3588 bytes) sent
69 elements cleared
linecard in sync after reloading
0/0/0 xdr elements in LowQ/MediumQ/HighQ
11/9/69 peak elements on LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0
CEF Table statistics:
Table name          Version Prefix-xdr Status
Default-table       7          4 Active, up, sync

CEF linecard slot number 1, status up
Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
Send failed 0, Out Of Sequence 0, drops 0
Linecard CEF reset 0, reloaded 1
95 elements packed in 6 messages(3588 bytes) sent
69 elements cleared
linecard in sync after reloading
0/0/0 xdr elements in LowQ/MediumQ/HighQ
11/9/69 peak elements on LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0
CEF Table statistics:
Table name          Version Prefix-xdr Status
Default-table       7          4 Active, up, sync
```

The following is sample output from the **show cef linecard internal** command for all line cards:

```
Router# show cef linecard internal
```

```
CEF linecard slot number 0, status up
Sequence number 11, Maximum sequence number expected 35
Send failed 0, Out Of Sequence 0
Linecard CEF reset 2, reloaded 2
Total elements queued:
prefix              4
adjacency           4
interface           91
address             2
policy routing      2
hw interface        57
state               6
resequence          2
control            13
```



```

table                2
time                4484
flow features deactivate 2
flow cache config    2
flow export config   2
dss                  2
isl                  2
mpls atm vc remove   2
mpls atm vc set label 2
                    2
                    2
                    3
                    1
4574 elements packed in 4495 messages(90286 bytes) sent
115 elements cleared
Total elements cleared:
prefix                2
adjacency             1
interface             63
address               1
policy routing        1
hw interface          29
state                 2
control               5
table                 1
flow features deactivate 1
flow cache config     1
flow export config    1
dss                   1
isl                   1
mpls atm vc remove    1
mpls atm vc set label 1
                    1
                    1
                    1
linecard disabled - failed a reload
0/0/0 xdr elements in LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0

CEF Table statistics:
Table name          Version Prefix-xdr Status
Default-table       8          4 Active, sync

```

Table 17 describes the significant fields shown in the displays.

Table 17 *show cef linecard Field Descriptions*

Field	Description
Table name	Name of the Cisco Express Forwarding table.
Version	Number of the Forwarding Information Base (FIB) table version.
Prefix-xdr	Number of prefix IPC information elements external data representation (XDRs) processed.
Status	State of the Cisco Express Forwarding table.
Slot	Slot number of the line card.
MsgSent	Number of interprocess communications (IPC) messages sent.
XDRSent	XDRs packed into IPC messages sent from the Route Processor (RP) to the line card.

Table 17 *show cef linecard Field Descriptions (continued)*

Field	Description
Window	Size of the IPC window between the line card and the RP.
LowQ/MedQ/HighQ	Number of XDR elements in the Low, Medium, and High priority queues.
Flags	Indicates the status of the line card. States are: • up—Line card is up. • sync—Line card is in synchronization with the main FIB. • FIB is repopulated on the line card. • reset—Line card FIB is reset. • reloading—Line card FIB is being reloaded. • disabled—Line card is disabled.
CEF-XDR	Number of Cisco Express Forwarding XDR messages processed.
I/Fs	Interface numbers.

Related Commands

Command	Description
show cef	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.

show cef memory

To display information about Cisco Express Forwarding memory usage, use the **show cef memory** command in privileged EXEC mode.

show cef memory [**changes** | **chunk-utilisation** [**changes** | **summary** [**changes**]] | **snapshot** | **summary**]

Syntax Description	changes	Displays Cisco Express Forwarding memory usage changes since the last snapshot.
	chunk-utilisation	Displays Cisco Express Forwarding chunk memory utilization.
	summary	Displays a summary of Cisco Express Forwarding memory usage.
	snapshot	Displays Cisco Express Forwarding memory information and takes a snapshot.

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 monitor the memory usage of Cisco Express Forwarding processes. You can display a summary of Cisco Express Forwarding memory usage, display a snapshot of memory use, and display changes to memory use since the last snapshot was taken.
-------------------------	--

Examples	The following is sample output from the show cef memory command:
-----------------	---

Router# **show cef memory**

Memory		in use/allocated	Count
ADJ: NULL adjacency	:	276/328 (84%)	[1]
ADJ: adj sev context	:	208/312 (66%)	[2]
ADJ: adjacency	:	856/960 (89%)	[2]
ADJ: request resolve	:	2200/2304 (95%)	[2]
ADJ: sevs	:	256/360 (71%)	[2]
CEF: FIB subtree context	:	28/80 (35%)	[1]
CEF: FIBHWIDB	:	19440/20480 (94%)	[20]
CEF: FIBIDB	:	6352/7392 (85%)	[20]
CEF: FIBWSB control	:	496/600 (82%)	[2]
CEF: IPv4 ARP throttle	:	1028/1080 (95%)	[1]
CEF: IPv4 not-sw cnt	:	76/128 (59%)	[1]
CEF: IPv4 not-sw si	:	76/128 (59%)	[1]

```

CEF: OCE get hash callbac :          28/80          ( 35%) [1]
CEF: Table rate Monitor S :          88/192          ( 45%) [2]
CEF: arp throttle chunk   :    22096/22200          ( 99%) [2]
CEF: dQ elems             :    208/312             ( 66%) [2]
CEF: fib                  :    1640/1744            ( 94%) [2]
CEF: fib GSB              :    2496/2808            ( 88%) [6]
CEF: fib deps             :    208/312             ( 66%) [2]
CEF: fib_fib_s            :    456/560             ( 81%) [2]
CEF: fib_fib_src_interfac :    208/312             ( 66%) [2]
CEF: fib_fib_src_special_ :    208/312             ( 66%) [2]
CEF: fib_rib_route_update :    4840/4944            ( 97%) [2]
CEF: fibhwidb table       :    40004/40056          ( 99%) [1]
CEF: fibidb table         :    40004/40056          ( 99%) [1]
CEF: hash table           :    262152/262256          ( 99%) [2]
CEF: ipv6 feature error c :    1260/1312            ( 96%) [1]
CEF: ipv6 feature error s :    1260/1312            ( 96%) [1]
CEF: ipv6 not cef switche :    484/536             ( 90%) [1]
CEF: ipv6 not cef switche :    484/536             ( 90%) [1]
CEF: loadinfos            :    504/608             ( 82%) [2]
CEF: mpls long path exts  :    280/384             ( 72%) [2]
CEF: mpls path exts       :    200/304             ( 65%) [2]
CEF: nh entry context     :    280/384             ( 72%) [2]
CEF: non_ip entry context :    280/384             ( 72%) [2]
CEF: pathl                :    2424/2736            ( 88%) [6]
CEF: pathl ifs            :    280/384             ( 72%) [2]
CEF: pathl its            :    352/456             ( 77%) [2]
CEF: pathloutputchain     :    432/536             ( 80%) [2]

```

Table 18 describes the significant fields shown in the display.

Table 18 *show cef memory Field Descriptions*

Field	Description
Memory	The type of Cisco Express Forwarding process that is using memory.
in use/allocated	Number of bytes in use by Cisco Express Forwarding and the number of bytes allocated for use by Cisco Express Forwarding.
Count	Number of blocks in use.
ADJ	Indicates a Cisco Express Forwarding adjacency process.
CEF	Indicates a Cisco Express Forwarding process.

The following is sample output from the **show cef memory summary** command:

```
Router# show cef memory summary
```

```
CEF has allocated 502888 bytes of memory (7904 bytes overhead)
```

This example shows that Cisco Express Forwarding allocated 502888 bytes of memory. The difference between the amount of memory in use and the amount of memory allocated is 7904 bytes.

The following is sample output from the **show cef memory snapshot** command:

```
Router# show cef memory snapshot
```

```
CEF memory snapshot taken at 00:26:01.116
```

This example shows when you last took a snapshot of Cisco Express Forwarding memory.

The following is sample output from the **show cef memory changes** command:

```
Router# show cef memory changes
```

```
No changes in CEF memory allocation in last 00:36:05.064
```

This examples shows the Cisco Express Forwarding memory changes, if any, that have occurred since the last memory snapshot was taken.

Related Commands

Command	Description
show cef	Displays information about packets forwarded by Cisco Express Forwarding.

show cef not-cef-switched



Note

The **show cef not-cef-switched** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases.

To display which packets were sent to a different switching path, use the **show cef not-cef-switched** command in user EXEC or privileged EXEC mode.

show cef not-cef-switched

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Support for multiple platforms was added.
12.0(22)S	The display output for this command was modified to include support for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 packets.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. Previously there was a show cef command, and drop was a keyword of that command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2S releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Usage Guidelines

If packets are not being cef switched and you want to determine why, enter the **show cef not-cef-switched** command.

**Note**

If Cisco Express Forwarding for IPv6 or distributed Cisco Express Forwarding for IPv6 is enabled globally on the router, the **show cef not-cef-switched** command displays IPv6 Cisco Express Forwarding counter information and IPv4 Cisco Express Forwarding counter information. If Cisco Express Forwarding for IPv6 or distributed Cisco Express Forwarding for IPv6 is not enabled globally on the router, the command displays only IPv4 Cisco Express Forwarding counter information.

Examples

The following is sample output from the **show cef not-cef-switched** command:

Router# **show cef not-cef-switched**

```
CEF Packets passed on to next switching layer
Slot No_adj No_encap Unsupp'ted Redirect Receive Options Access Frag
RP      0      0      0      0      91584      0      0      0
1       0      0      0      0       0      0      0      0
2       0      0      0      0       0      0      0      0

IPv6 CEF Packets passed on to next switching layer
Slot No_adj No_encap Unsupp'ted Redirect Receive Options Access MTU
RP      0      0      0      0      92784      0      0      0
1       0      0      0      0       0      0      0      0
2       0      0      0      0       0      0      0      0
```

Table 19 describes the significant fields shown in the display.

Table 19 *show cef not-cef-switched Field Descriptions*

Field	Meaning
Slot	The slot number on which the packets were received.
No_adj	Indicates the number of packets sent to the processor due to incomplete adjacency.
No_encap	Indicates the number of packets sent to the processor for Address Resolution Protocol (ARP) resolution.
Unsupp'ted	Indicates the number of packets punted to the next switching level due to unsupported features.
Redirect	Records packets that are ultimately destined to the router, and packets destined to a tunnel endpoint on the router. If the decapsulated tunnel is IP, it is Cisco Express Forwarding switched; otherwise, packets are process switched.
Receive	Indicates the number of packets ultimately destined to the router, or packets destined to a tunnel endpoint on the router. If the decapsulated tunnel packet is IP, the packet is Cisco Express Forwarding switched. Otherwise, packets are process switched.
Options	Indicates the number of packets with options. Packets with IP options are handled only at the process level.
Access	Indicates the number of packets punted due to an access list failure.

Table 19 *show cef not-cef-switched Field Descriptions (continued)*

Field	Meaning
Frag	Indicates the number of packets punted due to fragmentation failure. Note This field is not supported for IPv6 packets.
MTU	Indicates the number of packets punted due to maximum transmission unit (MTU) failure. Note This field is not supported for IPv4 packets.

Related Commands

Command	Description
show cef drop	Displays a list of which packets each line card dropped.
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.

show cef state

To display the state of Cisco Express Forwarding on a networking device, use the **show cef state** command in privileged EXEC mode.

show cef state

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.0(22)S	This command was introduced on Cisco 7500, 10000, and 12000 series Internet routers.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S on Cisco 7500 series routers.
	12.2(20)S	Support for the Cisco 7304 router was added. The Cisco 7500 series router is not supported in Cisco IOS Release 12.2(20)S.
	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.

Examples **Example for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and Later Releases**
The following example shows the state of Cisco Express Forwarding on the active Route Processor (RP):

```
Router# show cef state

CEF Status:
  RP instance
  common CEF enabled
IPv4 CEF Status:
  CEF enabled/running
  dCEF disabled/not running
  CEF switching enabled/running
  universal per-destination load sharing algorithm, id A189DD49
IPv6 CEF Status:
  CEF enabled/running
  dCEF disabled/not running
  original per-destination load sharing algorithm, id A189DD49
```

Table 20 describes the significant fields shown in the display.

Table 20 *show cef state Field Description (New)*

Field	Description
RP instance	Cisco Express Forwarding status is for the RP.
common CEF enabled	Common Cisco Express Forwarding is enabled.
IPv4 CEF Status	Cisco Express Forwarding mode and status is for IPv4.
universal per-destination load sharing algorithm	IPv4 is using the universal per-destination load sharing algorithm for Cisco Express Forwarding traffic.
IPv6 CEF Status	Cisco Express Forwarding mode and status is for IPV6.
original per-destination load sharing algorithm	IPv6 is using the original per-destination load sharing algorithm for Cisco Express Forwarding traffic.

Example for Cisco IOS Releases Before Cisco IOS 12.2(25)S

The following example shows the state of Cisco Express Forwarding on the active Route Processor (RP):

```
Router# show cef state
```

```
RRP state:
  I am standby RRP:          no
  RF Peer Presence:          yes
  RF PeerComm reached:       yes
  Redundancy mode:           SSO(7)
  CEF NSF:                   enabled/running
```

[Table 21](#) describes the significant fields shown in the display.

Table 21 *show cef state Field Descriptions*

Field	Description
I am standby RRP: no	This RP is not the standby.
RF Peer Presence: yes	This RP does have RF peer presence.
RF PeerComm reached: yes	This RP has reached RF peer communication.
Redundancy mode: SSO(&)	Type of redundancy mode on this RP.
CEF NSF: enabled/running	States whether Cisco Express Forwarding nonstop forwarding (NSF) is running or not.

The following example shows the state of Cisco Express Forwarding on the standby RP:

```
Router# show cef state
```

```
RRP state:
  I am standby RRP:          yes
  My logical slot:           0
  RF Peer Presence:          yes
  RF PeerComm reached:       yes
  CEF NSF:                   running
```

Related Commands

Command	Description
clear ip cef epoch	Begins a new epoch and increments the epoch number for a Cisco Express Forwarding table.
show cef nsf	Displays the current NSF state of Cisco Express Forwarding on both the active and standby RPs.

show cef subtree context client

To display Cisco Express Forwarding prefix subtrees, use the **show cef subtree context client** command in privileged EXEC mode.

```
show cef subtree context client {all | ip-session | test}
```

Syntax Description

all	Displays all Cisco Express Forwarding clients that provide prefix subtree context.
ip-session	Displays Cisco Express Forwarding IP sessions that provide prefix subtree context.
test	Tests all Cisco Express Forwarding applications that provide prefix subtree context.

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



Note

This command is for debugging purposes only. Do not use it unless instructed to do so by a Cisco service engineer.

Examples

The following example shows how to display information about all clients that provide subtree context:

```
Router# show cef subtree context client all

Client: FIB_SC: Test
  instances: 0
  app space: 0
  platform space: 0
```

[Table 22](#) describes the significant fields shown in the display.

Table 22 *show cef subtree context client all Field Descriptions*

Field	Description
FIB_SC: Test	Identifies the name of the client. This is useful information for the Cisco service engineer.
instances: 0	Number of instances of the subtree context.
app space: 0	Amount of extra space requested by the application for each instance of the subtree context.
platform space: 0	Amount of extra space requested by the platform for each instance of the subtree context.

Related Commands

Command	Description
show cef	Displays information about packets forwarded by Cisco Express Forwarding.

show cef table

To display the configuration and operational state of the Cisco Express Forwarding Forwarding Information Base (FIB) table, use the **show cef table** command in privileged EXEC mode.

Cisco IOS 12.2(33)SRB and Later S-Based Releases

```
show cef table [consistency-check | detail | internal | [ipv4 | ipv6] [vrf { * | Default | vrf-name }]]
               [topology { * | base | topology-name }] [detail | internal]]
```

Cisco IOS 12.4(20)T and Later T-Based Releases

```
show cef table [consistency-check | detail | internal | [ipv4 | ipv6] {Default | vrf-name} [detail |
internal]]
```

Syntax Description

consistency-check	(Optional) Displays the status of consistency checkers in the FIB.
detail	(Optional) Displays detailed Cisco Express Forwarding operational status and configuration.
internal	(Optional) Displays internal Cisco Express Forwarding operational status and configuration.
ipv4	(Optional) Displays operational status for IPv4 from the IPv4 FIB.
ipv6	(Optional) Displays operational status for IPv6 from the IPv6 FIB.
vrf	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance for the specified address family.
*	Displays operational status for all configured VRFs (vrf *) or all topologies (topology *), respectively.
Default	Displays operational status for the default VRF for the specified address family.
<i>vrf-name</i>	Displays operational status for the named VRF configured for the specified address family.
topology	(Optional) Specifies a topology for the selected address family.
base	Displays operational status for the base topology for the specified address family.
<i>topology-name</i>	Displays operational status for the identified topology-specific table.

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 2.2(28)SB.
12.2(33)SRA	This command was introduced.
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 the configuration and operational statistics for Cisco Express Forwarding IPv4 FIB and IPv6 FIB.

Cisco IOS 12.4(20)T and Later T-based Releases

When you enter an **ipv4** or **ipv6** keyword with the **show cef table** command, you must enter the name of a configured VRF or the **Default** keyword.

Cisco IOS 12.2(33)SRB and Later S-based Releases

The **vrf** and **topology** keywords are optional when you enter the **ipv4** or **ipv6** keyword with the **show cef table** command.

Examples

The following is sample output from the **show cef table** command:

```
Router# show cef table

Global information:
Output chain build favors:
  platform:      not configured
  CLI:           not configured
  operational:   convergence-speed
Output chain build characteristics:
  Inplace modify
    operational for:  load-sharing
  Collapse
    operational for:  load-sharing
  Indirection
    operational for:  recursive-prefix
MTRIE information:
TAL: node pools:
  pool[C/8 bits]: 12 allocated (0 failed), 12480 bytes {1 refcount}

1 active IPv4 table (9 prefixes total) out of a maximum of 10000.
VRF          Prefixes      Memory  Flags
Default          9         13520

1 active IPv6 table (1 prefix total) out of a maximum of 10000.
VRF          Prefixes      Memory  Flags
VRF          Prefixes      Memory  Flags
Default          1          208
```

Table 23 describes significant fields shown in the display.

Table 23 *show cef table Field Descriptions*

Field	Description
Output chain build favors:	Indicates table output chain building operational preferences.
Platform: not configured	Output chain building characteristics are not explicitly set or supported by the platform. The default output chain building characteristics are used.
CLI: not configured	Output chain building characteristics are not explicitly configured. The default is used.
operational: convergence speed	Output chain building favors convergence. This is the default operational behavior.

Table 23 *show cef table Field Descriptions (continued)*

Field	Description
Output chain build characteristics	Indicates the output chain building characteristics.
Inplace modify operational for: load-sharing	Indicates that the load sharing information in effect can be changed if the output information of the Interior Gateway Protocol (IGP) changes.
Collapse operational for: load-sharing	Indicates that the load-sharing tree is collapsed if load balancing is not affected.
Indirection operational for: recursive-prefix	Indicates that the use of indirection objects is enabled for recursive prefixes.
MTRIE information:	Indicates that information about the multi-array retrieval (MTRIE) follows.
TAL: node pools:	Indicates that node pool information for the Tree Abstraction Layer (TAL) follows.
pool (C/8 bits):	Indicates the memory management technique for the pool and the stride size (8 bits). The C indicates the use of a chunk pool. An M would indicate the use of a malloc.

The following is sample output from the **show cef table internal** command:

```
Router# show cef table internal

Table: IPv4:Default (id 0)
sources:           Default table
ref count:         31
flags (0x00):      none
smp allowed:        yes
default network:    none
route count:        9
route count (fwd):  9
route count (non-fwd): 0
Database epoch:     0 (9 entries at this epoch)
Subblocks:

  These rates are ndbs/minute.
  RIB update rate:   0
  RIB update peak rate: 0
Internals:
table:              0x4BFA060
extra:              0x000000
broker record:      0x000000
tal root:           0x4C01988
lookup OCE:         0x4C12B50

Table: IPv6:Default (id 0)
sources:           Default table
ref count:         3
flags (0x00):      none
smp allowed:        no
default network:    none
route count:        1
route count (fwd):  1
route count (non-fwd): 0
Database epoch:     0 (1 entry at this epoch)
```


Subblocks:

These rates are ndbs/minute.
 RIB update rate: 0
 RIB update peak rate: 0

Internals:

table: 0x4BF9FF0
 extra: 0x000000
 broker record: 0x000000
 tal root: 0x4C96328
 lookup OCE: 0x4C12B30

Table 24 describes significant fields shown in the display.

Table 24 *show cef table internal Field Descriptions*

Field	Description
Table: IPv4: Default (id 0)	The FIB table, IPv4 or IPv6, for which operation statistics follow.
sources: Default table	The source of the information comes from the Default table.
ref count: 3	The number of internal pointers to the VRF table structure.
flags (0x00): none	No flags are configured.
smp allowed: yes	Symmetrical Multi-Processing (SMP) is allowed.
default network: none	A default network is not configured.
route count: 9	Total number of routes is 9.
route count (fwd): 9	The number of routes forwarded is 9.
route count (non-fwd): 0	The number of routes not forwarded is 0.
Database epoch: 0 (9 entries at this epoch)	Epoch number (table version) is 0 and contains 9 entries.
Subblocks:	No subblocks are defined.
RIB update rate: 0	No update rate is configured for the RIB.
RIB update peak rate 0	No peak update rate is defined for the RIB.
Internal:	Identification for Cisco Express Forwarding internal operations.

The following is sample output from the **show cef table consistency-check** command:

Router# **show cef table consistency-check**

Consistency checker master control: enabled

IPv4:

Table consistency checker state:
 scan-rib-ios: disabled
 0/0/0/0 queries sent/ignored/checked/iterated
 scan-ios-rib: disabled
 0/0/0/0 queries sent/ignored/checked/iterated
 full-scan-rib-ios: enabled [1000 prefixes checked every 60s]
 0/0/0/0 queries sent/ignored/checked/iterated
 full-scan-ios-rib: enabled [1000 prefixes checked every 60s]
 0/0/0/0 queries sent/ignored/checked/iterated
 Checksum data checking disabled

```

Inconsistency error messages are disabled
Inconsistency auto-repair is enabled (10s delay, 300s holddown)
Inconsistency auto-repair runs: 0
Inconsistency statistics: 0 confirmed, 0/16 recorded

```

IPv6:

```

Table consistency checker state:
  scan-ios-rib: disabled
    0/0/0/0 queries sent/ignored/checked/iterated
  full-scan-rib-ios: enabled [1000 prefixes checked every 60s]
    0/0/0/0 queries sent/ignored/checked/iterated
  full-scan-ios-rib: enabled [1000 prefixes checked every 60s]
    0/0/0/0 queries sent/ignored/checked/iterated
Checksum data checking disabled
Inconsistency error messages are disabled
Inconsistency auto-repair is enabled (10s delay, 300s holddown)
Inconsistency auto-repair runs: 0
Inconsistency statistics: 0 confirmed, 0/16 recorded

```

Table 25 describes significant fields shown in the display.

Table 25 *show cef table consistency-check Field Descriptions*

Field	Description
scan-rib-ios: disabled	The consistency checker that compares the Routing Information Base (RIB) to the FIB table and provides the number of entries missing from the FIB table is disabled.
scan-ios-rib: disabled	The consistency checker that compares the FIB table to the RIB and provides the number of entries missing from the RIB is disabled.
full-scan-rib-ios: enabled	A full scan is enabled that compares the RIB to the FIB table. Every 60 seconds, 1000 prefixes are checked.
full-scan-ios-rib: enabled	A full scan is enabled that compares the FIB table to the RIB. Every 60 seconds, 1000 prefixes are checked.
Checksum data checking disabled	The data-checking function is disabled.
Inconsistency error messages are disabled	The consistency checker to generate inconsistency error messages is disabled.
Inconsistency auto-repair is enabled (10s delay, 300s holddown)	The auto repair function is enabled with the default settings of a 10-second delay and a 300-second holddown.

The following is sample output from the **show cef table IPv4 Default** command:

```

Router# show cef table ipv4 Default

Table: IPv4:Default (id 0)
sources:          Default table
ref count:        31
flags (0x00):     none
smp allowed:      yes
default network:  none
route count:      9
route count (fwd): 9
route count (non-fwd): 0
Database epoch:   0 (9 entries at this epoch)
Subblocks:

```

```

These rates are ndbs/minute.
RIB update rate:          0
RIB update peak rate:     0

```

For a description of significant fields shown in the display, see [Table 24](#).

The following is sample output from the **show cef table IPv6 Default internal** command:

```

Router# show cef table ipv6 Default internal

Table: IPv6:Default (id 0)
sources:                Default table
ref count:              3
flags (0x00):          none
smp allowed:            no
default network:        none
route count:            1
route count (fwd):      1
route count (non-fwd):  0
Database epoch:         0 (1 entry at this epoch)
Subblocks:

These rates are ndbs/minute.
RIB update rate:        0
RIB update peak rate:   0
Internals:
table:                  0x4BF9FF0
extra:                  0x000000
broker record:          0x000000
tal root:               0x4C96328
lookup OCE:             0x4C12B30

```

For a description of significant fields shown in the display, see [Table 24](#).

Related Commands

Command	Description
cef table consistency-check	Enables Cisco Express Forwarding table consistency checker types and parameters.
cef table output-chain build	Configures Cisco Express Forwarding table output chain building characteristics for the forwarding of packet through the network.
show cef	Displays information about packets forwarded by Cisco Express Forwarding.

show cef table download priority

To display the configured download priority of Cisco Express Forwarding routes, use the **show cef table download priority** command in privileged EXEC mode.

show cef table download priority

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SRE	This command was introduced.

Usage Guidelines

Use this command to display the configured priority for Cisco Express Forwarding routes that are downloaded from the Route Processor (RP) to the line cards.

You can change the default priority for a route type with the **cef table download** configuration command. If you change the default priority for a route type, the **show cef table download priority** command displays the user-configured priority followed by the default priority in parentheses.

Examples

The following sample output shows the configured download priority of the routes and prefixes from the Cisco Express Forwarding table on the RP to the line cards:

```
Router# show cef table download priority

Route type                                priority
Route with recursive dependents          1st
Default route, 0.0.0.0/0 or ::/0         1st
Directly connected route                 2nd
Receive route, local address on router   2nd
Route is in a VRF                        3rd
Any other route not matched              4th
```

This example shows that the default download priorities are in effect.

[Table 26](#) describes the significant fields shown in the display.

Table 26 show cef table download priority Field Descriptions

Field	Description
Route type	Type of route in the Cisco Express Forwarding table downloaded from the RP to the line cards.
priority	Order in which the route type is downloaded from the RP to the line cards.

In the following example, the default priority of a default route and a receive route was changed with the **cef table download** command:

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# cef table download default-route priority 2
```

```
Router(config)# cef table download receive-route priority 4
```

```
Router(config)# exit
```

The following **show cef table download priority** command displays the newly configured download priority and the default priority (in parentheses) for the default route and the receive route:

```
Router# show cef table download priority
```

```
Route type                                priority
Route with recursive dependents           1st
Default route, 0.0.0.0/0 or ::/0         2nd (default 1st)
Directly connected route                  2nd
Receive route, local address on router    4th (default 2nd)
Route is in a VRF                         3rd
Any other route not matched               4th
```

See [Table 26](#) for a description of the significant fields shown in the display.

Related Commands

Command	Description
cef table download	Sets download characteristics for prefixes and routes in the Cisco Express Forwarding table.

show cef timers

To display the current state of the timers internal to the Cisco Express Forwarding process, use the **show cef timers** command in user EXEC or privileged EXEC mode.

show cef timers

Syntax Description This command has no arguments or keywords.

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

Command History	Release	Modification
	12.3(2)T	This command was introduced.
	12.2(25)S	Command output was changed.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Examples **Example for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and Later Releases**

The following is sample output from the **show cef timer** command:

```
Router# show cef timers

CEF background process
  Expiration    Type
    13.248  (parent)
    13.248  FIB checkers: IPv4 scan-rib-ios scanner
    13.248  FIB checkers: IPv4 scan-ios-rib scanner
    13.248  FIB checkers: IPv6 scan-ios-rib scanner

Platform counter polling is not enabled
IPv4 CEF background process
  Expiration    Type
    0.600  (parent)
    0.600  ARP throttle
    0.600  adjacency update hwidb
```

[Table 27](#) describes the significant fields shown in the display.

Table 27 *show cef timers Field Descriptions*

Field	Description
Expiration	Seconds in which the timers will expire
Type	Identification of the counter

Example for Cisco IOS Releases Before Cisco IOS Release 12.2(25)S

The following is sample output from the **show cef timers** command:

```
Router# show cef timers
```

```

CEF background process
  Expiration  Type
    0.208 (parent)
    0.208 adjacency update hwidb
    0.540 slow resolution
    1.208 ARP throttle

CEF FIB scanner process
  Expiration  Type
    44.852 (parent)
    44.852 checker scan-rib

```

Table 28 describes the significant fields shown in the display.

Table 28 *show cef timers Field Descriptions*

Field	Description
Expiration	Seconds in which the timers will expire
Type	Identification of the timer

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.

show cef vrf

To display information about Cisco Express Forwarding Virtual Private Networks (VPN) routing and forwarding (VRF) instances, use the **show cef vrf** command in privileged EXEC mode.

```
show cef vrf [ipv4 | ipv6] [Default | vrf-name]
```

Syntax Description	ipv4	(Optional) Displays IPv4 address-family type VRF instances.
	ipv6	(Optional) Displays IPv6 address-family type VRF instances.
	Default	(Optional) Default VRF for the specified address family.
	vrf-name	(Optional) Name assigned to a VRF.

Command Default If you do not specify any arguments or keywords, the command displays information about all VRFs in the Cisco Express Forwarding Forwarding Information Base (FIB).

Command Modes Privileged EXEC (#)

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

Usage Guidelines Use this command to display information about specified VRF instances or all VRF instances in the Cisco Express Forwarding FIB. To display information about all VRF instances in the FIB, omit arguments and keywords.

Examples The following is sample output from the **show cef vrf** command:

```
Router# show cef vrf

AF: IPv4, VRF: Default(0)
  Contains 1 table:
    IPv4:Default
AF: IPv6, VRF: Default(0)
  Contains 1 table:
    IPv6:Default
```

[Table 29](#) describes significant fields shown in the display.

Table 29 *show cef vrf Field Descriptions*

Field	Description
AF: IPv4	The address-family type is IPv4.
VRF: Default (0)	Identifies the default VRF.
AF: IPv6	The address-family type is IPv6.

The following is sample output from the **show cef vrf ipv4** command:

```
Router# show cef vrf ipv4
```

```
AF: IPv4, VRF: Default(0)
  Contains 1 table:
    IPv4:Default
```

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

```
Router# show cef vrf ipv6
```

```
AF: IPv6, VRF: Default(0)
  Contains 1 table:
    IPv6:Default
```

For a description of significant fields in the displays, see [Table 29](#).

Related Commands

Command	Description
show cef	Displays information about packets forwarded by Cisco Express Forwarding.

show interface stats

To display numbers of packets that were process switched, fast switched, and distributed switched, use the **show interface stats** command in user EXEC or privileged EXEC mode.

show interface *type number* **stats**

Syntax Description

<i>type number</i>	Interface type and number about which to display statistics.
--------------------	--

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.3(14)YM2	This command was modified to show the counter for Multi-Processor Forwarding (MPF) switched packets.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)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.

Usage Guidelines

Use this command on the Route Processor (RP).



Note

When fast switching is configured on the outbound interface, and RSP optimum, RSP flow, and VIP DFS switching modes are all specified on the incoming interface, the interface on which RSP optimum, RSP flow, and VIP DFS switching modes is not enabled can still show packets switched out via those switching paths when packets are received from other interfaces with RSP optimum, RSP flow, and VIP DES switching modes enabled.

Examples

The following sample output is from Cisco IOS Release 12.3(14)YM2 and shows counters for both Multi-Processor Forwarding (MPF) switched packets on native GigabitEthernet interfaces and for non-MPF FastEthernet interfaces:

Router# **show interface stats**

```
GigabitEthernet0/0
  Switching path  Pkts In  Chars In  Pkts Out  Chars Out
    Processor           0         0       225       77625
    Route cache         0         0         0         0
  Multi-Processor Fwding   950      221250     500      57000
    Total             950      221250     725     134625
GigabitEthernet0/1
  Switching path  Pkts In  Chars In  Pkts Out  Chars Out
```

```

        Processor          1          60          226          77685
        Route cache        0           0           0           0
    Multi-Processor Fwding    500       57000          500       57000
        Total              501       57060          726       134685
GigabitEthernet0/2
    Switching path      Pkts In    Chars In    Pkts Out    Chars Out
        Processor        1           60          226          77685
        Route cache      0           0           0           0
    Multi-Processor Fwding    0           0           0           0
        Total            1           60          226          77685
FastEthernet1/0
    Switching path      Pkts In    Chars In    Pkts Out    Chars Out
        Processor      34015       5331012         1579       158190
        Route cache    0           0           0           0
        Total          34015       5331012         1579       158190

```

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

Router# **show interface fddi 3/0/0 stats**

```

Fddi3/0/0
    Switching path      Pkts In    Chars In    Pkts Out    Chars Out
        Processor      3459994  1770812197    4141096  1982257456
        Route cache    10372326  3693920448     439872   103743545
    Distributed cache    19257912  1286172104    86887377  1184358085
        Total          33090232  2455937453    91468345  3270359086

```

[Table 30](#) describes the significant fields in the display.

Table 30 *show interface stats Field Descriptions*

Field	Description
Fddi3/0/0	Interface for which information is shown
Switching path	Column heading for the various switching paths below it
Pkts In	Number of packets received in each switching mechanism
Chars In	Number of characters received in each switching mechanism
Pkts Out	Number of packets sent out each switching mechanism
Chars Out	Number of characters sent out each switching mechanism

show interfaces switching

To display the number of packets sent and received on an interface classified by the switching path, use the **show interfaces switching** command in user EXEC and privileged EXEC mode.

show interfaces [*type number*] **switching**

Syntax Description

<i>type number</i>	Interface type and number about which to display packet switching path information.
--------------------	---

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

Use the **show interfaces switching** command to show which path the router uses and how the traffic is switched. This command is also useful for troubleshooting CPU utilization.

Statistics for packets in, bytes in, packets out, and bytes out are displayed for the available protocols. The statistics are arranged by process, cache misses, fast-path, and autonomous path. All values displayed by the **show interfaces switching** command are absolute. The **clear interface counters** command has no effect on these values.

You must enter at least seven characters of the **switching** keyword (**switchi**) when you use the **show interfaces switching** command.

Examples

The following shows sample output from the **show interfaces switching** command:

```
Router# show interfaces switching
```

```
FastEthernet0/0
  Throttle count      0
    Drops            RP      0      SP      0
  SPD Flushes        Fast    0      SSE      0
  SPD Aggress        Fast    0
  SPD Priority      Inputs    0      Drops      0

  Protocol IP
    Switching path   Pkts In   Chars In   Pkts Out   Chars Out
      Process        24      8208        0          0
    Cache misses      0          -          -          -
      Fast           0          0          0          0
    Auton/SSE         0          0          0          0

  Protocol DECnet
    Switching path   Pkts In   Chars In   Pkts Out   Chars Out
      Process         0          0          0          0
    Cache misses      0          -          -          -
      Fast           0          0          0          0
```

```

Auton/SSE          0          0          0          0
.....
.....

Protocol IPv6
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Process           0          0          0          0
Cache misses      0          -          -          -
Fast              0          0          0          0
Auton/SSE         0          0          0          0

Protocol Other
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Process           2          120         3          180
Cache misses      0          -          -          -
Fast              0          0          0          0
Auton/SSE         0          0          0          0

```

NOTE: all counts are cumulative and reset only after a reload.

Interface POS4/0 is disabled

The following shows sample output from the **show interfaces switching** command for the interface FastEthernet 0/0:

Router> **show interfaces FastEthernet 0/0 switching**

```

FastEthernet0/0
  Throttle count      0
    Drops             RP          0          SP          0
    SPD Flushes       Fast        218         SSE          0
    SPD Aggress       Fast         0
    SPD Priority      Inputs        0          Drops        0

Protocol IP
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Process           239        23422        237        23226
Cache misses      0          -          -          -
Fast              0          0          0          0
Auton/SSE         0          0          0          0

Protocol ARP
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Process           4          240         3          180
Cache misses      0          -          -          -
Fast              0          0          0          0
Auton/SSE         0          0          0          0

Protocol CDP
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Process           8          2632        15          5477
Cache misses      0          -          -          -
Fast              0          0          0          0
Auton/SSE         0          0          0          0

```

NOTE: all counts are cumulative and reset only after a reload.

Table 31 describes the significant fields shown in the display.

Table 31 *show interfaces switching Field Descriptions*

Field	Description
Throttle count	Number of times input packet processing was throttled on this interface.
Drops	RP—Number of packets dropped for input congestion. SP—Number of packets flushed by external throttling.
SPD Flushes	Fast—Number of packets flushed by selective packet discard on RP. SSE—Number of packets flushed by external selective packet discard.
SPD Aggress	Fast—Input packets dropped by aggressive selective packet discard.
SPD Priority	Inputs—Number of priority packets received. Drops—Number of priority packets dropped.
Protocol	Name of the protocol for which packet switching information is displayed.
Switching Path	Indicates the traffic switching path.
Pkts In	Number of incoming packets.
Chars In	Number of incoming bytes.
Pkts Out	Number of outgoing packets.
Chars Out	Number of outgoing bytes.
Process	Process switching. With this type of switching, an incoming packet is associated with a destination network or subnet entry in the routing table located in main memory. Process switching is performed by the system processor.
Cache misses	Packets that were forwarded through the process level (for which there was no entry in fast switching cache).
Fast	Fast switching. With this type of switching, an incoming packet matches an entry in the fast-switching cache located in main memory. Fast switching is done via asynchronous interrupts, which are handled in real time. Fast switching allows higher throughput by switching a packet using a cache created by previous packets.
Auton	Autonomous switching. With this type of switching, an incoming packet matches an entry in the autonomous-switching cache located on the interface processor. Autonomous switching provides faster packet switching by allowing the ciscoBus controller to switch packets independently without having to interrupt the system processor. It is available only on Cisco 7000 series routers and in AGS+ systems with high-speed network controller cards.
SSE	Silicon switching engine switching. With this type of switching, an incoming packet matches an entry in the silicon-switching cache located in the silicon switching engine (SSE) of the Silicon Switch Processor (SSP) module. This module is available only on Cisco 7000 series routers. Silicon switching provides very fast, dedicated packet switching by allowing the SSE to switch packets independently without having to interrupt the system processor.

Related Commands

Command	Description
show interface stats	Displays numbers of packets that were process switched, fast switched, and distributed switched.

show ip cache

To display the routing table cache used to fast switch IP traffic, use the **show ip cache** command in user EXEC or privileged EXEC mode.

show ip cache [*prefix mask*] [*type number*]

Syntax Description	<i>prefix mask</i>	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
	<i>type number</i>	(Optional) Displays only the entries in the cache that match the interface type and number combination.

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

Command History	Release	Modification
	10.0	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	The show ip cache display shows MAC headers up to 92 bytes.
-------------------------	--

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

Router# **show ip cache**

```
IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last 7 seconds, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago
```

Prefix/Length	Age	Interface	MAC Header
131.108.1.1/32	0:01:09	Ethernet0/0	AA000400013400000C0357430800
131.108.1.7/32	0:04:32	Ethernet0/0	00000C01281200000C0357430800
131.108.1.12/32	0:02:53	Ethernet0/0	00000C029FD000000C0357430800
131.108.2.13/32	0:06:22	Fddi2/0	00000C05A3E000000C035753AAAA0300 00000800
131.108.2.160/32	0:06:12	Fddi2/0	00000C05A3E000000C035753AAAA0300 00000800
131.108.3.0/24	0:00:21	Ethernet1/2	00000C026BC600000C03574D0800
131.108.4.0/24	0:02:00	Ethernet1/2	00000C026BC600000C03574D0800
131.108.5.0/24	0:00:00	Ethernet1/2	00000C04520800000C03574D0800
131.108.10.15/32	0:05:17	Ethernet0/2	00000C025FF500000C0357450800

131.108.11.7/32	0:04:08	Ethernet1/2	00000C010E3A00000C03574D0800
131.108.11.12/32	0:05:10	Ethernet0/0	00000C01281200000C0357430800
131.108.11.57/32	0:06:29	Ethernet0/0	00000C01281200000C0357430800

Table 32 describes the significant fields shown in the display.

Table 32 *show ip cache Field Descriptions*

Field	Description
IP routing cache version	Version number of this table. This number is incremented any time the table is flushed.
entries	Number of valid entries.
bytes	Number of bytes of processor memory for valid entries.
hash overflows	Number of times autonomous switching cache overflowed.
Minimum invalidation interval	Minimum time delay between cache invalidation request and actual invalidation.
maximum interval	Maximum time delay between cache invalidation request and actual invalidation.
quiet interval	Length of time between cache flush requests before the cache will be flushed.
threshold <n> requests	Maximum number of requests that can occur while the cache is considered quiet.
Invalidation rate <n> in last <m> seconds	Number of cache invalidations during the last <m> seconds.
0 in last 3 seconds	Number of cache invalidation requests during the last quiet interval.
Last full cache invalidation occurred <hh:mm:ss> ago	Time since last full cache invalidation was performed.
Prefix/Length	Network reachability information for cache entry.
Age	Age of cache entry.
Interface	Output interface type and number.
MAC Header	Layer 2 encapsulation information for cache entry.

The following is sample output from the **show ip cache** command with a prefix and mask specified:

```
Router# show ip cache 131.108.5.0 255.255.255.0
```

```
IP routing cache version 4490, 119 entries, 17464 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:11:56 ago
```

```
Prefix/Length      Age      Interface      MAC Header
131.108.5.0/24    0:00:34  Ethernet1/2    00000C04520800000C03574D0800
```

The following is sample output from the **show ip cache** command with an interface specified:

Router# **show ip cache e0/2**

```
IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago
```

Prefix/Length	Age	Interface	MAC Header
131.108.10.15/32	0:05:17	Ethernet0/2	00000C025FF500000C0357450800

Related Commands

Command	Description
clear ip cache	Deletes entries in the routing table cache used to fast switch IP traffic.

show ip cef

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

Privileged EXEC Mode

```
show ip cef [[[network [network-mask] | network/mask] [longer-prefixes] | interface-type number]
[platform] [detail | internal [checksum]] | [network [network-mask] | network/mask]
[dependents | same-routing] | prefix-statistics]
```

User EXEC Mode

```
show ip cef [[[network [network-mask] | network/mask] [longer-prefixes] | interface-type number]
[platform] [detail] | [network [network-mask] | network/mask] [dependents | same-routing] |
prefix-statistics]
```

Syntax Description	
<i>network</i>	(Optional) Network number for which to display a FIB entry.
<i>network-mask</i>	(Optional) Network mask to be used with the specified <i>network</i> value.
<i>network/mask</i>	(Optional) The network number assigned to the interface and the length of the prefix.
longer-prefixes	(Optional) Displays FIB entries for more specific destinations.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
platform	(Optional) Displays platform-specific data structure only.
detail	(Optional) Displays detailed FIB entry information.
internal	(Optional) Displays the FIB internal data structure. The internal keyword is available in privileged EXEC mode only.
checksum	(Optional) Displays FIB entry checksum values. The checksum keyword is available in privileged EXEC mode only.
dependents	(Optional) Displays all prefixes recursing through the FIB.
same-routing	(Optional) Displays all prefixes with the same routing.
prefix-statistics	(Optional) Displays nonzero prefix statistics.

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

Command History	Release	Modification
	11.2GS	This command was introduced on the Cisco 12012 Internet router.
	11.1CC	This command was modified. Multiple platform support was added.

Release	Modification
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.0(17)ST	This command was modified. The display of a message indicating support for Border Gateway Protocol (BGP) policy accounting was added.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was modified. The checksum , internal , platform , and prefix-statistics keywords were added. Output was changed to show IPv4 output only.
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(24)T	This command was modified. The dependents , longer-prefixes , and same-routing keywords were added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use of the **show ip cef** command without any keywords or arguments shows a brief display of all FIB entries.

The **show ip cef detail** command shows detailed FIB entry information for all FIB entries.

Examples

The following is sample output from the **show ip cef detail** command for Ethernet interface 0. It shows all the prefixes resolving through adjacency pointing to next hop Ethernet interface 0/0 and next hop interface IP address 192.0.2.233.

```
Router# show ip cef Ethernet 0/0 detail
```

```
IP Distributed CEF with switching (Table Version 136808)
45800 routes, 8 unresolved routes (0 old, 8 new) 45800 leaves, 2868 nodes, 8444360 bytes,
136808 inserts, 91008 invalidations 1 load sharing elements, 208 bytes, 1 references 1 CEF
resets, 1 revisions of existing leaves refcounts: 527343 leaf, 465638 node

172.16.0.0/12, version 7417, cached adjacency 192.0.2.230 0 packets, 0 bytes,
Adjacency-prefix
via 192.0.2.231, Ethernet0/0, 0 dependencies
next hop 192.0.2.232, Ethernet0/0
valid cached adjacency
```

[Table 33](#) describes the significant fields shown in the display.

Table 33 *show ip cef detail Field Descriptions*

Field	Description
routes	Total number of entries in the Cisco Express Forwarding table.
unresolved routes	Number of entries in the Cisco Express Forwarding table that do not have resolved recursions categorized by old and new routes.
leaves, nodes, bytes	Number of elements in the Cisco Express Forwarding table and how much memory they use.
inserts	Number of nodes inserted.

Table 33 *show ip cef detail Field Descriptions (continued)*

Field	Description
invalidations	Number of entries that have been invalidated.
load sharing elements, bytes, references	Information about load sharing elements: how many, number of associated bytes, and number of associated references.
CEF resets	Number of times the Cisco Express Forwarding table has reset.
revisions of existing leaves refcounts	Number of revisions of the existing elements in the Cisco Express Forwarding table.
version	Version of the Cisco Express Forwarding table.
cached adjacency	Type of adjacency to which this Cisco Express Forwarding table entry points.
packets, bytes	Number of packets and bytes switched through the name entry.
dependencies	Number of table entries that point to the named entry.
next hop	Type of adjacency or the next hop toward the destination.

The following is sample output from the **show ip cef detail** command for the prefix 192.0.2.1, showing that the BGP policy accounting bucket number 4 (traffic_index 4) is assigned to this prefix:

```
Router# show ip cef 192.0.2.1 detail

192.168.5.0/24, version 21, cached adjacency to POS7/2
0 packets, 0 bytes, traffic_index 4
via 192.0.2.233, 0 dependencies, recursive
next hop 192.0.2.234, POS7/2 via 172.16.0.0/12
valid cached adjacency
```

[Table 33](#) describes the significant fields shown in the display.

Related Commands

Command	Description
show cef	Displays the packets dropped by the line cards, or displays the packets that were not express forwarded.
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef summary	Displays a summary of the entries in the IPv6 FIB.

show ip cef adjacency

To display Cisco Express Forwarding and distributed Cisco Express Forwarding recursive and direct prefixes resolved through an adjacency, use the **show ip cef adjacency** command in user EXEC or privileged EXEC mode.

```
show ip cef [vrf vrf-name] adjacency interface-type interface-number ip-prefix [checksum | detail | epoch epoch-number | internal | platform | source]
```

To display Cisco Express Forwarding and distributed Cisco Express Forwarding recursive and direct prefixes resolved through special adjacency types representing nonstandard switching paths, use this form of the **show ip cef adjacency** command in user EXEC or privileged EXEC mode.

```
show ip cef [vrf vrf-name] adjacency {discard | drop | glean | null | punt} [detail] [checksum | detail | epoch epoch-number | internal | platform | source]
```

For Cisco 10000 Series Routers

To display Cisco Express Forwarding and recursive and direct prefixes resolved through an adjacency, use the **show ip cef adjacency** command in user EXEC or privileged EXEC mode.

```
show ip cef [vrf vrf-name] adjacency interface-type interface-number ip-prefix [detail | internal | platform]
```

To display Cisco Express Forwarding and recursive and direct prefixes resolved through special adjacency types representing nonstandard switching paths, use the **show ip cef adjacency** command in user EXEC or privileged EXEC mode.

```
show ip cef [vrf vrf-name ] adjacency {discard | drop | glean | null | punt} [detail] [internal] [platform]
```

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>interface-type</i> <i>interface-number</i>	Interface type and number for which to display Forwarding Information Base (FIB) entries.
<i>ip-prefix</i>	Next-hop IP prefix, in dotted decimal format (A.B.C.D).
checksum	(Optional) Displays FIB entry checksums.
detail	(Optional) Displays detailed information for each Cisco Express Forwarding adjacency type entry.
epoch <i>epoch-number</i>	(Optional) Displays adjacency type entries filtered by epoch number. The epoch number range is from 0 to 255.
internal	(Optional) Displays data for adjacency type entries.
platform	(Optional) Displays platform-specific adjacency information.
source	(Optional) Displays source-specific adjacency information.
discard	Discard adjacency. Sets up the adjacency for loopback interfaces. Loopback IP addresses are receive entries in the FIB table.
drop	Drop adjacency. Packets forwarded to this adjacency are dropped.

glean	Glean adjacency. Represents destinations on a connected interface for which no Address Resolution Protocol (ARP) cache entry exists.
null	Null adjacency. Formed for the null 0 interface. Packets forwarded to this adjacency are dropped.
punt	Punt adjacency. Represents destinations that cannot be switched in the normal path and that are punted to the next-fastest switching vector.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)T	The vrf keyword was added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The internal , platform , and source keywords were added.
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

An adjacency is a node that can be reached by one Layer 2 hop.

Examples

The following is sample output from the **show ip cef adjacency** command when the **glean** keyword is specified:

```
Router# show ip cef adjacency glean
```

Prefix	Next Hop	Interface
10.2.61.0/24	attached	Ethernet1/0/0
10.17.250.252/32	10.2.61.1	Ethernet1/0/0

The following is sample output from the **show ip cef adjacency drop** command with the **detail** keyword specified:

```
Router# show ip cef adjacency drop detail
```

```
IP CEF with switching (Table Version 4), flags=0x0
 4 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 0
 4 leaves, 8 nodes, 8832 bytes, 13 inserts, 9 invalidations
 0 load sharing elements, 0 bytes, 0 references
universal per-destination load sharing algorithm, id 00B999CA
 3 CEF resets, 0 revisions of existing leaves
Resolution Timer: Exponential (currently 1s, peak 1s)
 0 in-place modifications
refcounts: 533 leaf, 536 node
```

```

10.0.0.0/4, version 3
0 packets, 0 bytes, Precedence routine (0)
  via 0.0.0.0, 0 dependencies
    next hop 0.0.0.0
    valid drop adjacency

```

The following sample output shows the direct IP prefix when the next hop Gigabit Ethernet interface 3/0 is specified:

```
Router# show ip cef adjacency GigabitEthernet 3/0 172.20.26.29
```

```

Prefix          Next Hop          Interface
10.1.1.0/24      10.20.26.29      GigabitEthernet3/0

```

Cisco 10000 Series Routers Examples Only

The **show ip cef adjacency** command shows all prefixes resolved through a regular next-hop adjacency or through the usage of a special adjacency type keyword such as **discard**, **drop**, **glean**, **null**, or **punt**.

The following is sample output from the **show ip cef adjacency** command when the **glean** keyword is specified:

```
Router# show ip cef adjacency glean
```

```

Prefix          Next Hop          Interface
10.2.61.0/24      attached          GigabitEthernet1/0/0
10.17.250.252/32  10.2.61.1        GigabitEthernet1/0/0

```

The following is sample output from the **show ip cef adjacency drop** command with the **detail** keyword specified:

```
Router# show ip cef adjacency drop detail
```

```

IPv4 CEF is enabled for distributed and running
VRF Default:
  42 prefixes (42/0 fwd/non-fwd)
  Table id 0
  Database epoch: 3 (42 entries at this epoch)

```

```

10.0.0.0/4, epoch 3
  Special source: drop
  drop

```

The following sample output shows the direct IP prefix when the next hop Gigabit Ethernet interface 3/0/0 is specified (before Cisco IOS Release 12.2(25)S):

```
Router# show ip cef adjacency GigabitEthernet 3/0/0 172.20.26.29
```

```

Prefix          Next Hop          Interface
10.1.1.0/24      10.20.26.29      GigabitEthernet3/0/0

```

[Table 34](#) describes the significant fields shown in the display.

Table 34 *show ip cef adjacency Field Descriptions (Before Cisco IOS Release 12.2(25)S)*

Field	Description
Prefix	Destination IP prefix.
Next Hop	Next hop IP address.
Interface	Next hop interface.

For Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases the information in the output is the same, but the format of the output is changed.

```
Router# show ip cef adjacency FastEthernet 0/1 172.17.22.1
```

```
10.10.1.2/32
  nexthop 172.17.22.1 FastEthernet0/1
10.20.12.0/24
  nexthop 172.17.22.1 FastEthernet0/1
```

Table 35 describes the significant fields shown in the display.

Table 35 *show ip cef adjacency Field Descriptions*

Field	Description
10.10.1.2/32	Destination IP prefix.
nexthop 172.17.22.1	Next hop IP address.
FastEthernet0/1	Next hop interface.

Related Commands

Command	Description
show adjacency	Displays Cisco Express Forwarding adjacency table information.
show ip cef summary	Displays a summary of the entries in the FIB.
show ipv6 adjacency	Displays Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 recursive and direct prefixes resolved through an adjacency.

show ip cef epoch

To display the epoch information for all Forwarding Information Base (FIB) tables, use the **show ip cef epoch** command in user EXEC or privileged EXEC mode

show ip cef epoch

Syntax Description This command has no arguments or keywords.

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(25)S	Table adjacency epoch information was moved from the output of this command to the output of the show adjacency prefix command.
	12.2(28)SB	This command was integrated into the Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into the Cisco IOS Release 12.2(33)SRA
	12.2(33) SXH	This command was integrated into the Cisco IOS Release 12.2(33)SXH.
	12.4(20)T	This command was integrated into the Cisco IOS Release 12.4(20)T.

Usage Guidelines These **show** commands also display the epoch information for the following:

- **show ip cef summary**—Displays the table epoch for a specific FIB table.
- **show ip cef detail**—Displays the epoch value for each entry of a specific FIB table.
- **show adjacency summary**—Displays the adjacency table epoch.
- **show adjacency detail**—Displays the epoch value for each entry of the adjacency table.

Examples **Sample Output for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and Later Releases**
This example shows how to display epoch information. The fields shown in the display are self-explanatory.

```
Router# show ip cef epoch
```

```
VRF: Default
Database epoch: 0 (12 entries at this epoch)
```

For adjacency table epoch information, see the **show adjacency prefix** command.

Sample Output for Cisco IOS Releases Before Cisco IOS Release 12.2(25)S

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

```
Router# show ip cef epoch
```

```
CEF epoch information:
```

```
Table:Default-table
```

```
Table epoch:2 (164 entries at this epoch)
```

```
Adjacency table
```

```
Table epoch:1 (33 entries at this epoch)
```

This example shows the output after you clear the epoch table and increment the epoch number. The fields shown in the display are self-explanatory.

```
Router# show ip cef epoch
```

```
CEF epoch information:
```

```
Table:Default-table
```

```
Table epoch:2 (164 entries at this epoch)
```

```
Adjacency table
```

```
Table epoch:1 (33 entries at this epoch)
```

```
Router# clear ip cef epoch full
```

```
Router# show ip cef epoch
```

```
CEF epoch information:
```

```
Table:Default-table
```

```
Table epoch:3 (164 entries at this epoch)
```

```
Adjacency table
```

```
Table epoch:2 (33 entries at this epoch)
```

Related Commands

Command	Description
show ip cef	Displays entries in the FIB or displays a summary of the FIB.
show ip cef summary	Displays a summary of the FIB.
show ip cef detail	Displays detailed FIB entry information.
show adjacency detail	Displays the information about the protocol detail and timer.
show adjacency summary	Displays a summary of Cisco Express Forwarding adjacency information.

show ip cef events



Note

The **show ip cef events** command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases.

To display all recorded Cisco Express Forwarding Forwarding Information Base (FIB) and adjacency events, use the **show ip cef events** command in user EXEC or privileged EXEC mode.

show ip cef [**vrf** *vrf-name*] **events** [*ip-prefix*] [**new** | **within** *seconds*] [**detail**] [**summary**]

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>ip-prefix</i>	(Optional) Next hop IP prefix, in dotted decimal format (A.B.C.D).
new	(Optional) Displays new Cisco Express Forwarding events not previously shown.
within <i>seconds</i>	(Optional) Displays Cisco Express Forwarding events that occurred within a specified number of seconds.
detail	(Optional) Displays detailed information for each Cisco Express Forwarding event entry.
summary	(Optional) Displays a summary of the Cisco Express Forwarding event log.

Command Modes

User EXEC (>)
Privileged EXEC(#)

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(28)SB	This command was removed. It is not available in Cisco IOS Release 12.2(28)SB and later Cisco IOS 12.2SB releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.2(33)SXH	This command was removed. It is not available in Cisco IOS Release 12.2(33)SXH and later Cisco IOS 12.2S releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Usage Guidelines

This command shows the state of the table event log and must be enabled for events to be recorded. The **ip cef table event-log** command controls parameters such as event log size.

Examples

The following is sample output from the **show ip cef events** command with **summary** specified:

```
Router# show ip cef events summary

CEF table events summary:
  Storage for 10000 events (320000 bytes), 822/0 events recorded/ignored
  Matching all events, traceback depth 16
  Last event occurred 00:00:06.516 ago.
```

The following is sample output from the **show ip cef events** command displaying events that occurred within 1 second:

```
Router# show ip cef events within 1

CEF table events (storage for 10000 events, 14 events recorded)
+00:00:00.000:[Default-table] *.*.*.*/*          New FIB table          [OK]
+00:00:00.000:[Default-table] 10.1.80.194/32      FIB insert in mtrie    [OK]
+00:00:00.000:[Default-table] 10.1.80.0/32        FIB insert in mtrie    [OK]
+00:00:00.000:[Default-table] 10.1.80.255/32      FIB insert in mtrie    [OK]
+00:00:00.004:[Default-table] 10.1.80.0/24        FIB insert in mtrie    [OK]
+00:00:00.004:[Default-table] 10.1.80.0/24        NBD up                 [OK]
+00:00:00.004:[Default-table] 224.0.0.0/8         FIB insert in mtrie    [OK]
+00:00:00.012:[Default-table] 10.1.80.0/24        NBD up                 [Ignr]
+00:00:00.012:[Default-table] 224.0.0.0/8         FIB remove             [OK]
+00:00:00.016:[Default-table] 224.0.0.0/8         FIB insert in mtrie    [OK]
+00:00:05.012:[Default-table] 224.0.0.0/8         FIB remove             [OK]
+00:00:05.012:[Default-table] 224.0.0.0/8         FIB insert in mtrie    [OK]
+00:00:28.440:[Default-table] 224.0.0.0/8         FIB remove             [OK]
+00:00:28.440:[Default-table] 224.0.0.0/8         FIB insert in mtrie    [OK]
First event occurred at 00:00:36.568 (00:04:40.756 ago)
Last event occurred at 00:01:05.008 (00:04:12.316 ago)
```

Table 36 describes the significant fields shown in the display.

Table 36 *show ip cef events Field Descriptions*

Field	Description
+00:00:00.000	Time stamp of the IP Cisco Express Forwarding event.
[Default-table]	Type of VRF table for this event entry.
..*.*/*	All IP prefixes.
9.1.80.194/32	IP prefix associated with the event.
FIB insert in mtrie	IP prefix insert in the FIB table event.
NBD up	IP prefix up event.
FIB remove	FIB entry remove event.
[Ignr]	Cisco Express Forwarding ignored event.
[OK]	Cisco Express Forwarding processed event.

Related Commands

Command	Description
ip cef table consistency-check	Enables Cisco Express Forwarding table consistency checker types and parameters.
ip cef table event-log	Controls Cisco Express Forwarding table event-log characteristics.

show ip cef exact-route

To display the exact route for a source-destination IP address pair, use the **show ip cef exact-route** command in user EXEC or privileged EXEC mode.

```
show ip cef [vrf vrf-name] exact-route source-address [src-port port-number] destination-address
[dest-port port-number]
```

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>source-address</i>	The network source address.
src-port	(Optional) Specifies a source port.
<i>port-number</i>	(Optional) The Layer 4 port number of the source IP address, if configured. The port number can be from 0 to 65535.
<i>destination-address</i>	The network destination address.
dest-port	(Optional) Specifies a destination port.
<i>port-number</i>	(Optional) The Layer 4 port number of the destination IP address, if configured. The port number can be from 0 to 65535.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(4)T	This command was introduced.
12.2(25)S	Command output was reformatted.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The src-port <i>port-number</i> and dest-port <i>port-number</i> keywords and arguments were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

When you are load balancing per destination, this command shows the exact next hop that is used for a given IP source-destination pair.

If you configured the **ip cef load-sharing algorithm include-ports** command and the **source**, **destination**, or **source destination** keywords, you can use the source port number or the destination port number or both port numbers to see the load-balancing decision for a source and destination address. These options are available only if the include-ports algorithm is enabled.

Examples

Sample Output for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and Later Releases

The following is sample output from the **show ip cef exact-route** command:

```
Router# show ip cef exact-route 172.16.1.3 172.16.1.2

172.16.1.3 -> 172.16.1.2 => IP adj out of FastEthernet0/1, addr 172.17.25.1
```

[Table 37](#) describes the significant fields shown in the display.

Table 37 *show ip cef exact-route Field Descriptions*

Field	Description
172.16.1.3 -> 172.16.1.2	From source 172.16.1.3 to destination 172.16.1.2.
FastEthernet0/1,	Next hop is out interface FastEthernet0/1.
addr 172.17.25.1	IP address of the next hop is 172.17.25.1.

Sample Output for Cisco IOS Releases Before Cisco IOS Release 12.2(25)S

The following is sample output from the **show ip cef exact-route** command:

```
Router# show ip cef exact-route 10.1.1.1 172.17.249.252

10.1.1.1          -> 172.17.249.252 :Ethernet2/0/0 (next hop 10.1.104.1)
```

[Table 38](#) describes the significant fields shown in the display.

Table 38 *show ip cef exact-route Field Descriptions*

Field	Description
10.1.1.1 -> 172.17.249.252	From source 10.1.1.1 to destination 172.17.249.252.
Ethernet2/0/0 (next hop 10.1.104.1)	Next hop is 10.1.104.1 on Ethernet 2/0/0.

Related Commands

Command	Description
ip cef load-sharing algorithm	Selects a Cisco Express Forwarding load-balancing algorithm.

show ip cef inconsistency



Note

The `show ip cef inconsistency` command is not available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases. This command is replaced by the **test cef table consistency** command.

To display Cisco Express Forwarding IP prefix inconsistencies, use the **show ip cef inconsistency** command in user EXEC or privileged EXEC mode.

show ip cef [**vrf** *vrf-name*] **inconsistency** [**records** [**detail**]]

Syntax Description	vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
	<i>vrf-name</i>	(Optional) Name assigned to the VRF.
	records	(Optional) Displays all recorded inconsistencies.
	detail	(Optional) Displays detailed information for each Cisco Express Forwarding table entry.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(15)S	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
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 12.2(17d)SXB.
12.2(25)S	This command was removed. It is not available in Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
12.2(33)SRA	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRA and later Cisco IOS 12.2SR releases.
12.4(20)T	This command was removed. It is not available in Cisco IOS Release 12.4(20)T and later Cisco IOS 12.4T releases.

Usage Guidelines

This command is available only on routers with line cards.

This command displays recorded IP Cisco Express Forwarding inconsistency records found by the lc-detect, scan-rp, scan-rib, and scan-lc detection mechanisms.

You can configure the IP Cisco Express Forwarding prefix consistency-detection mechanisms using the **cef table consistency-check** command.

Examples

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

```
Router# show ip cef inconsistency

Table consistency checkers (settle time 65s)
lc-detect:running
  0/0/0 queries sent/ignored/received
scan-lc:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
scan-rp:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
scan-rib:running [1000 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
Inconsistencies:0 confirmed, 0/16 recorded
```

Table 39 describes the significant fields shown in the display.

Table 39 *show ip cef inconsistency Field Descriptions*

Field	Description
settle time	Time after a recorded inconsistency is confirmed.
lc-detect running	Consistency checker lc-detect is running.
0/0/0 queries	Number of queries sent, ignored, and received.
Inconsistencies:0 confirmed, 0/16 recorded	Number of inconsistencies confirmed, and recorded. Sixteen is the maximum number of inconsistency records to be recorded.

Related Commands

Command	Description
clear ip cef inconsistency	Clears the statistics and records for the Cisco Express Forwarding consistency checker.
cef table consistency-check	Enables Cisco Express Forwarding table consistency checker types and parameters.

show ip cef non-recursive

To display nonrecursive route entries in the Forwarding Information Base (FIB), use the **show ip cef non-recursive** command in user EXEC or privileged EXEC mode.

show ip cef non-recursive [**detail** | **epoch** *epoch-number* | **internal** | **platform** | **source**]

Cisco 10000 Series Routers

show ip cef non-recursive [**detail** | **internal** | **platform**]

Syntax Description

detail	(Optional) Displays detailed nonrecursive route entry information.
epoch <i>epoch-number</i>	(Optional) Displays adjacency type entries filtered by epoch number. The epoch number range is from 0 to 255.
internal	(Optional) Displays data for nonrecursive route entries.
platform	(Optional) Displays platform-specific nonrecursive route entries.
source	(Optional) Displays source-specific nonrecursive route entry information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
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(25)S	The epoch , internal , platform , and source keywords were added, and the <i>epoch-number</i> argument was added.
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

The **show ip cef non-recursive detail** command shows detailed FIB entry information for all nonrecursive routes.

Examples

The following is sample output from the **show ip cef non-recursive detail** command:

```
Router# show ip cef non-recursive detail

IPv6 CEF is enabled and running
IPv6 CEF default table
8 prefixes
2001:xx::/35
    nexthop FE80::ssss:CFF:FE3D:DCC9 Tunnel155
2001:zzz:500::/40
    nexthop FE80::nnnn:801A Tunnel132
2001:zzz::/35
    nexthop 3FFE:mmm:8023:21::2 Tunnel126
3FFE:yyy:8023:37::1/128 Receive
    Receive
3FFE:yyy:8023:37::/64 Attached, Connected
    attached to Tunnel137
3FFE:yyy:8023:38::1/128 Receive
    Receive
3FFE:yyy:8023:38::/64 Attached, Connected
    attached to Tunnel140
3FFE:yyy:8023:39::1/128 Receive
    Receive
```

Cisco 10000 Series Router Example

The following is sample output from the **show ip cef non-recursive detail** command:

```
Router# show ip cef non-recursive detail

IPv4 CEF is enabled for distributed and running
VRF Default:
  42 prefixes (42/0 fwd/non-fwd)
  Table id 0
  Database epoch: 3 (42 entries at this epoch)

0.0.0.0/0, epoch 3, flags default route handler
  no route
0.0.0.0/32, epoch 3, flags receive
  Special source: receive
  receive
10.2.2.2/32, epoch 3
  local label info: global/24
  nexthop 10.1.1.1 GigabitEthernet1/0/0 label 18
10.4.4.4/32, epoch 3
  local label info: global/30
  nexthop 10.1.1.1 GigabitEthernet1/0/0 label 19
10.5.5.5/32, epoch 3
  local label info: global/29
  nexthop 10.1.1.1 GigabitEthernet1/0/0
10.6.6.6/32, epoch 3, flags receive
  receive
10.1.1.0/24, epoch 3
  local label info: global/23
  nexthop 10.1.1.1 GigabitEthernet1/0/0 label 17
```

Table 40 describes the significant fields shown in the displays.

Table 40 *show ip cef non-recursive Field Descriptions*

Field	Description
8 prefixes	Indicates the total number of prefixes in the Cisco Express Forwarding table.
2001:xx::/35	Indicates the prefix of the remote network.
2001:zzz:500::/40 nexthop FE80::nnnn:801A Tunnel32	Indicates that prefix 2001:zzz:500::/40 is reachable through this next-hop address and interface.
attached to Tunnel37	Indicates that this prefix is a connected network on Tunnel interface 37.
Receive	Indicates that this prefix is local to the router.

Related Commands

Command	Description
show ip cef	Displays entries in the FIB.
show ip cef summary	Displays a summary of the entries in the FIB.
show ip cef unresolved	Displays unresolved entries in the FIB.

show ip cef platform

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

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

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

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

Command History	Release	Modification
	12.2 (28)SB	The command was introduced.

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

```
Router# show ip cef 10.4.4.4 platform
```

```
10.4.4.4/32
Fib Entry: 0xD6680610 XCM leaf from 0x50805550(RP) 0xA0805550(FP):
load_bal_or_adj[0] 0x0 load_bal_or_adj[1] 0x18 load_bal_or_adj[2] 0x1C
leaf points to an adjacency, index 0x607
ip_mask 0x0 as_number 0x0 precedence_num_loadbal_intf 0xF0 qos_group 0x0
Label object OCE Chain:
Label(0x12, real) Adjacency
c10k_label_data = 0x450467F8
tag_elt_addr = 0x50003038
ipv6_tag_elt_addr = 0x0
tag_index = 0x607
tt_tag_rew = 0x45046800
Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
mac_rewrite_index = 0x395, flags = 0x9
pktswitched = 0 byteswitched = 0
XCM Tag Rewrite: vcci = 0x9DA, fib_root = 0x0
mac_rewrite_index = 0x395, flags = 0x9
mac_index_extension = 0x0
XCM mac rewrite from index 0x395
mtu from 0x53800E54(RP) 0xA3800E54(FP)
frag_flags = 0x0
mtu = 1496
mac length 0x12 encap length 0x16 upd_offset=0x02FF
mac string start from bank4 0x32001CA8(RP)
0x82001CA8(FP)
mac string end from bank9 0x50801CA8(RP)
0xA0801CA8(FP)
Encap String: 0005DC387B180003A011A57881000002884700012000
```

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

show ip cef summary

To display a summary of the IP Cisco Express Forwarding table, use the **show ip cef summary** command in user EXEC or privileged EXEC mode.

show ip cef summary

Syntax Description This command has no arguments and keywords.

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(25)S	The command output was changed to display IPv4 forwarding information only.
	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.

Examples **Sample Output for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and Later Releases**
This is sample output for the **show ip cef summary** command for IPv4 information:

```
Router# show ip cef summary

IPv4 CEF is enabled and running
VRF Default:
  22 prefixes (22/0 fwd/non-fwd)
  Table id 0, 1 resets
  Database epoch: 0 (22 entries at this epoch)
```

[Table 41](#) describes the significant fields shown in the displays.

Table 41 *show ip cef summary Field Descriptions*

Field	Description
IPv4 CEF is enabled and running	Status of IPv4 Cisco Express Forwarding on the router.
22 prefixes (22/0 fwd/non-fwd)	Number of prefixes forwarded and not forwarded.

Table 41 *show ip cef summary Field Descriptions (continued)*

Field	Description
Table id 0, 1 resets	Forwarding table version and the number of times the table was reset.
Database epoch: 0 (22 entries at this epoch)	Database version and the number of entries in the database.

In Cisco IOS 12.2(25)S, IPv4 and IPv6 output was separated. To display Cisco Express Forwarding summary information for IPv6, use the **show ipv6 cef summary** command, for example:

```
Router# show ipv6 cef summary
```

```
IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
Table id 0, 0 resets
Database epoch: 0 (20 entries at this epoch)
```

Sample Output for Cisco IOS Releases Before Cisco IOS Release 12.2(25)S

This example shows how to display a summary of the IP Cisco Express Forwarding table:

```
Router# show ip cef summary
```

```
IP Distributed CEF with switching (Table Version 25), flags=0x0
 21 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 1
 21 leaves, 16 nodes, 19496 bytes, 36 inserts, 15 invalidations
 0 load sharing elements, 0 bytes, 0 references
universal per-destination load sharing algorithm, id 5163EC15
3(0) CEF resets, 0 revisions of existing leaves
Resolution Timer: Exponential (currently 1s, peak 1s)
0 in-place/0 aborted modifications
refcounts: 4377 leaf, 4352 node
```

```
Table epoch: 0 (21 entries at this epoch)
```

```
Adjacency Table has 9 adjacencies
```

[Table 42](#) describes the significant fields shown in the display.

Table 42 *show ip cef summary Field Descriptions*

Field	Description
routes	Total number of entries in the Cisco Express Forwarding table.
unresolved	Number of entries in the Cisco Express Forwarding table that do not have resolved recursions categorized by old and new routes.
peak	Highest number of unresolved recursions.
leaves, nodes, bytes	Number of elements in the Cisco Express Forwarding table and how much memory they use.
load sharing algorithm, id	Type of load sharing, whether the router is configured for per destination or per packet and the identifier.
Table epoch	Number indicating the version of a Cisco Express Forwarding table from 0 to 255.

Related Commands

Command	Description
show ip cef	Displays entries in the FIB or displays a summary of the FIB.
show ipv6 summary	Displays a summary of the entries in the IPv6 FIB.

show ip cef switching statistics

To display switching statistics in the Forwarding Information Base (FIB), use the **show ip cef switching statistics** command in privileged EXEC mode.

show ip cef switching statistics [feature]

Syntax Description

feature (Optional) The output is ordered by feature.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced. This command replaces the show cef drop and the show cef not-cef-switched commands.
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

If the optional **feature** keyword is not used, all switching statistics are displayed, without regard for feature order.

Examples

The following is sample output from the **show ip cef switching statistics** command:

```
Router# show ip cef switching statistics
```

Reason	Drop	Punt	Punt2Host
RP LES Packet destined for us	0	132248	0
RP LES Multicast	0	2	0
RP LES Link-local	0	33	0
RP LES Total	0	132283	0
Slot 4 Packet destined for us	0	129546	0
Slot 4 Link-local	0	31	0
Slot 4 Total	0	129577	0
All Total	0	261860	0

The following example shows how to display switching statistics for all features in a common format:

```
Router# show ip cef switching statistics feature
```

```
IPv4 CEF input features:
Path  Feature      Drop    Consume    Punt  Punt2Host  New i/f
LES   Access List   0        0          1      0          0
RSP   Access List   0        0          1      0          0
Slot 0 Access List 10        0          1      0          0
```

Slot 0 Verify Unicast	9	0	0	0	0
Slot 4 Verify Unicast	5	0	0	0	0
Total	24	0	3	0	0

IPv4 CEF output features:

Path	Feature	Drop	Consume	Punt	Punt2Host	New i/f
Total		0	0	0	0	0

IPv4 CEF post-encap features:

Path	Feature	Drop	Consume	Punt	Punt2Host	New i/f
Total		0	0	0	0	0

Cisco 10000 Series Router Examples

The following is sample output from the **show ip cef switching statistics** command:

Router# **show ip cef switching statistics**

Path	Reason	Drop	Punt	Punt2Host
RP LES	Packet destined for us	0	1115	0
RP LES	Total	0	1115	0
RP PAS	Packet destined for us	0	385	0
RP PAS	TTL expired	0	0	1833
RP PAS	Total	0	385	1833
All	Total	0	1500	1833

The following example shows how to display switching statistics for all features in a common format:

Router# **show ip cef switching statistics feature**

IPv4 CEF input features:

Path	Feature	Drop	Consume	Punt	Punt2Host	Gave route
Total		0	0	0	0	0

IPv4 CEF output features:

Path	Feature	Drop	Consume	Punt	Punt2Host	New i/f
Total		0	0	0	0	0

IPv4 CEF post-encap features:

Path	Feature	Drop	Consume	Punt	Punt2Host	New i/f
Total		0	0	0	0	0

[Table 43](#) describes the significant fields shown in the displays.

Table 43 *show ip cef switching statistics Field Descriptions*

Field	Description
Path	Switch path where the feature was executed. Available switch paths are platform-dependent. Following are example switch paths for the Cisco 7200 series router: • RIB—process switching with Cisco Express Forwarding assistance • (low-end switching [LES])—Cisco Express Forwarding switch path • PAS—Cisco Express Forwarding turbo switch path Following are example switch paths for the Cisco 7500 series router: • RIB—centralized process switching with Cisco Express Forwarding assistance • LES—centralized Cisco Express Forwarding switch path on the Route/Switch Processor (RSP) • RSP—centralized Cisco Express Forwarding turbo switch path on the RSP • Slot NN—distributed Cisco Express Forwarding turbo switch path on the Versatile Interface Processor (VIP) in the indicated slot number
Feature	Feature that returned the statistics.
Reason	Packet description.
Consume	Number of packets that the feature removed from the switch path (and will probably reintroduce to the switch path later). For example, with crypto with hardware acceleration, the feature might queue the packets to encryption and decryption; because hardware (and software) encryption is time-consuming, these packets are queued so the main processor can begin handling the next packet while the crypto module processes the removed packet. Also, for example, the feature might queue the packets for process switching through a private queue for that feature.
Drop	Number of packets dropped.
Punt	Number of packets that could not be switched in the normal path and were punted to the next-fastest switching vector.
Punt2Host	Number of packets that could not be switched in the normal path and were punted to the host. For switch paths other than a centralized turbo switch path, punt and punt2host function the same way. With punt2host from a centralized turbo switch path (PAS and RSP), punt will punt the packet to LES, but punt2host will bypass LES and punt directly to process switching.
New i/f	Number of packets for which the feature provided Cisco Express Forwarding with forwarding information (that is, bypassed the normal route lookup).

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ip cef	Displays entries in the FIB.
show ip route	Displays router advertisement information received from onlink routers.

show ip cef traffic prefix-length

To display Cisco Express Forwarding traffic statistics by prefix size, use the **show ip cef traffic prefix-length** command in user EXEC or privileged EXEC mode.

show ip cef [**vrf** *vrf-name*] **traffic prefix-length**

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)T	The vrf keyword was added.
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

This command is used to display Cisco Express Forwarding switched traffic statistics by destination prefix length. The **ip cef accounting prefix-length** command must be enabled for the counters to increment.

Examples

The following is sample output from the **show ip cef traffic prefix-length** command:

Router# **show ip cef traffic prefix-length**

IP prefix length switching statistics:

Prefix Length	Number of Packets	Number of Bytes
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
.		
.		
.		
28	0	0
29	0	0
30	0	0

31	0	0
32	0	0

Table 44 describes the significant fields shown in the display.

Table 44 *show ip cef traffic prefix-length Field Descriptions*

Field	Description
Prefix Length	Destination IP prefix length for Cisco Express Forwarding switched traffic.
Number of Packets	Number of packets forwarded for the specified IP prefix length.
Number of Bytes	Number of bytes transmitted for the specified IP prefix length.

Related Commands

Command	Description
ip cef accounting	Enables network accounting of Cisco Express Forwarding.

show ip cef tree

To display summary information on the default tree in the Forwarding Information Base (FIB), use the **show ip cef tree** command in user EXEC or privileged EXEC mode.

Cisco 7500 Series Routers

```
show ip cef tree [statistics | dependents [prefix-filter]]
```

Cisco 10000 Series Routers

```
show ip cef tree [statistics]
```

Syntax Description

statistics	(Optional) Displays the default tree statistics.
dependents	(Optional) Displays the dependents of the selected tree with optional prefix filter.
<i>prefix-filter</i>	(Optional) A prefix filter on the dependents of the selected tree.

Command Modes

User EXEC (>)
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

If none of the optional keywords or argument is used, all summary information on the default tree in the IP FIB is shown.

Examples

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

Cisco 7500 Series Router Example

```
Router# show ip cef tree
```

```
VRF Default tree information:
RTRIE storing IPv6 addresses
6 entries (6/0 fwd/non-fwd)
Forwarding & Non-forwarding tree:
6 inserts, 0 delete
8 nodes using 288 bytes
```


Table 45 describes the significant fields shown in the display for a Cisco 7500 series router.

Table 45 *show ip cef tree Field Descriptions*

Field	Description
RTRIE storing IPv6 addresses	Indicates the tree type as RTRIE.
6 entries (6/0 fwd/non-fwd)	Indicates total number of prefix entries as 6 forwarding and 0 nonforwarding entries.
Forwarding & Non-forwarding tree	Same tree is used for forwarding and nonforwarding.
6 inserts, 0 delete	Indicates that 6 entries were inserted and 0 entries were deleted from the tree.
8 nodes using 288 bytes	Indicates a total of 8 nodes using a total of 288 bytes of memory.
*calloc failures: <i>number</i> node	This line is not present in the example output. If this line is present in output, it indicates a memory allocation error at the indicated node.

Cisco 10000 Series Router Example

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

Router# **show ip cef tree**

```
VRF Default tree information:
MTRIE/MTRIE storing IPv4 addresses
42 entries (42/0 fwd/non-fwd)
Forwarding tree:
  Forwarding lookup routine: IPv4 mtrie generic
  82 inserts, 40 deletes
  8-4-6-6-4-4 stride pattern
  short mask protection enabled for <= 4 bits without process suspension
  42 leaves (1176 bytes), 76 nodes (15744 bytes)
  18576 total bytes
  leaf ops: 82 inserts, 40 deletes
  leaf ops with short mask protection: 3 inserts, 1 delete
  per-prefix length stats: lookup off, insert off, delete off
  refcounts: 2933 leaf, 2848 node
  node pools:
    pool[C/4 bits]: 46 allocated (0 failed), 5472 bytes
    pool[C/6 bits]: 29 allocated (0 failed), 9216 bytes
    pool[C/8 bits]: 1 allocated (0 failed), 1056 bytes
Non-Forwarding tree:
  122 inserts, 122 deletes
  8-4-6-6-4-4 stride pattern
  short mask protection enabled for <= 4 bits without process suspension
  0 leaves (0 bytes), 1 node (1040 bytes)
  2696 total bytes
  leaf ops: 122 inserts, 122 deletes
  leaf ops with short mask protection: 4 inserts, 4 deletes
  per-prefix length stats: lookup off, insert off, delete off
  refcounts: 0 leaf, 0 node
  node pools:
    pool[C/4 bits]: 0 allocated (0 failed), 0 bytes
    pool[C/6 bits]: 0 allocated (0 failed), 0 bytes
    pool[C/8 bits]: 1 allocated (0 failed), 1040 bytes
```

Table 46 describes the significant fields shown in the display for a Cisco 10000 series router.

Table 46 *show ip cef tree Field Descriptions—Cisco 10000 Series Router*

Field	Description
MTRIE storing IPv4 addresses	Indicates the tree type as MTRIE.
42 entries (42/0 fwd/ non-fwd)	Indicates total number of prefix entries as 42 forwarding and 0 nonforwarding entries.
Forwarding & Non-forwarding tree	Same tree is used for forwarding and nonforwarding.
82 inserts, 40 delete	Indicates that 82 entries were inserted and 40 entries were deleted from the tree.
76 nodes using 15744 bytes	Indicates a total of 76 nodes using a total of 15744 bytes of memory.
*calloc failures: <i>number</i> node	This line is not present in the example output. If this line is present in output, it indicates a memory allocation error at the indicated node.

Related Commands

Command	Description
show ip cef	Displays entries in the FIB.

show ip cef unresolved

To display unresolved entries in the Forwarding Information Base (FIB), use the **show ip cef unresolved** command in user EXEC or privileged EXEC mode.

show ip cef unresolved [**detail** | **epoch** *epoch-number* | **internal** | **platform** | **source**]

Cisco 10000 Series Routers

show ip cef unresolved [**detail** | **internal** | **platform**]

Syntax Description		
detail	(Optional)	Displays detailed FIB entry information.
epoch <i>epoch-number</i>	(Optional)	Displays the basic unresolved routes filtered by a specified epoch number. The epoch number range is from 0 to 255.
internal	(Optional)	Displays data structures for unresolved routes.
platform	(Optional)	Displays platform-specific information on unresolved routes.
source	(Optional)	Displays source-specific information on unresolved routes.

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

Command History	Release	Modification
	12.0(22)S	This command was introduced.
	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(25)S	The platform , source , and epoch keywords were added. The <i>epoch-number</i> argument was added. The output was changed to list only IPv4 unresolved prefixes.
	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	The show ip cef unresolved detail command displays detailed information for all unresolved FIB entries.
------------------	--

Examples

Sample Output for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and Later Releases

The following is sample output for the **show ip cef unresolved** command:

```
Router# show ip cef unresolved detail
```

Prefix	Next Hop	Interface
--------	----------	-----------

Nothing is displayed if no unresolved adjacencies exist. For information about unresolved prefixes for IPv6, use the **show ipv6 unresolved** command.

Sample Output for Cisco IOS Releases Before Cisco IOS Release 12.2(25)S

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

```
Router# show ip cef unresolved
```

```
IP Distributed CEF with switching (Table Version 136632)
45776 routes, 13 unresolved routes (0 old, 13 new)
45776 leaves, 2868 nodes, 8441480 bytes, 136632 inserts, 90856 invalidations
1 load sharing elements, 208 bytes, 1 references
1 CEF resets, 1 revisions of existing leaves
refcounts: 527292 leaf, 465617 node
10.214.0.0/16, version 136622
0 packets, 0 bytes
  via 172.17.233.56, 0 dependencies, recursive
  unresolved
10.215.0.0/16, version 136623
0 packets, 0 bytes
  via 172.17.233.56, 0 dependencies, recursive
  unresolved
10.218.0.0/16, version 136624
0 packets, 0 bytes
```

Cisco 10000 Series Router Example

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

```
Router# show ip cef unresolved
```

```
10.214.0.0/16, version 136622
0 packets, 0 bytes
  via 172.17.233.56, 0 dependencies, recursive
  unresolved
10.215.0.0/16, version 136623
0 packets, 0 bytes
  via 172.17.233.56, 0 dependencies, recursive
  unresolved
10.218.0.0/16, version 136624
0 packets, 0 bytes
```

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding interface information.
show ip cef	Displays entries in the FIB.
show ip cef summary	Displays a summary of the entries in the FIB.
show ipv6 unresolved	Displays unresolved entries in the IPv6 FIB.

show ip cef vlan

To display the information about the IP Cisco Express Forwarding VLAN interface status, the configuration, and the prefixes for a specific interface, use the **show ip cef vlan** command in user EXEC or privileged EXEC mode.

show ip cef vlan *vlan-id* [**detail**]

Syntax Description	<i>vlan-id</i>	VLAN number; valid values are from 1 to 4094.
	detail	(Optional) Displays the detailed information about the IP Cisco Express Forwarding VLAN interface.
Defaults	This command has no default settings.	
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.

Examples This example shows how to display the prefixes for a specific VLAN. The fields shown in the display are self-explanatory.

```
Router> show ip cef vlan 1003
```

```
Prefix           Next Hop           Interface
0.0.0.0/0         172.20.52.1        FastEthernet3/3
0.0.0.0/32         receive
10.7.0.0/16        172.20.52.1        FastEthernet3/3
10.16.18.0/23      172.20.52.1        FastEthernet3/3
Router>
```

This example shows how to display detailed IP Cisco Express Forwarding information for a specific VLAN. The fields shown in the display are self-explanatory.

```
Router> show ip cef vlan 1003 detail
```

```
IP Distributed CEF with switching (Table Version 2364), flags=0x0
 1383 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
 1383 leaves, 201 nodes, 380532 bytes, 2372 inserts, 989 invalidations
 0 load sharing elements, 0 bytes, 0 references
universal per-destination load sharing algorithm, id 9B6C9823
 3 CEF resets, 0 revisions of existing leaves
  refcounts: 54276 leaf, 51712 node
Adjacency Table has 5 adjacencies
```

show ip cef vrf

To display the Cisco Express Forwarding forwarding table associated with a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **show ip cef vrf** command in privileged EXEC mode.

```
show ip cef vrf vrf-name [ip-prefix [mask [longer-prefixes]] [detail] [output-modifiers]] [interface
interface-number] [adjacency [interface interface-number] [detail] [discard] [drop] [glean]
[null] [punt] [output-modifiers]] [detail [output-modifiers]] [non-recursive [detail]
[output-modifiers]] [summary [output-modifiers]] [traffic [prefix-length] [output-modifiers]]
[unresolved [detail] [output-modifiers]]
```

Syntax Description

<i>vrf-name</i>	Name assigned to the VRF.
<i>ip-prefix</i>	(Optional) IP prefix of entries to show, in dotted decimal format (A.B.C.D).
<i>mask</i>	(Optional) Mask of the IP prefix, in dotted decimal format.
longer-prefixes	(Optional) Displays table entries for all of the more specific routes.
detail	(Optional) Displays detailed information for each Cisco Express Forwarding table entry.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<i>interface</i>	(Optional) Type of network interface to use: ATM, Ethernet, Loopback, packet over SONET (POS) or Null.
<i>interface-number</i>	Number identifying the network interface to use.
adjacency	(Optional) Displays all prefixes resolving through adjacency.
discard	(Optional) Discards adjacency.
drop	(Optional) Drops adjacency.
glean	(Optional) Gleans adjacency.
null	(Optional) Nulls adjacency.
punt	(Optional) Punts adjacency.
non-recursive	(Optional) Displays only nonrecursive routes.
summary	(Optional) Displays a Cisco Express Forwarding table summary.
traffic	(Optional) Displays traffic statistics.
prefix-length	(Optional) Displays traffic statistics by prefix size.
unresolved	(Optional) Displays only unresolved routes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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.
12.2(33)SRE	This command was modified. Support for the BGP best external and BGP additional path features was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Used with only the *vrf-name* argument, the **show ip cef vrf** command shows a shortened display of the Cisco Express Forwarding table.

Used with the **detail** keyword, the **show ip cef vrf** command shows detailed information for all Cisco Express Forwarding table entries.

Examples

This example shows the forwarding table associated with the VRF called vrf1:

```
Router# show ip cef vrf vrf1
```

Prefix	Next Hop	Interface
0.0.0.0/32	receive	
10.11.0.0/8	10.50.0.1	Ethernet1/3
10.12.0.0/8	10.52.0.2	POS6/0
10.50.0.0/8	attached	Ethernet1/3
10.50.0.0/32	receive	
10.50.0.1/32	10.50.0.1	Ethernet1/3
10.50.0.2/32	receive	
10.50.255.255/32	receive	
10.51.0.0/8	10.52.0.2	POS6/0
10.224.0.0/24	receive	
10.255.255.255/32	receive	

The following sample output from the **show ip cef vrf vrf-name ip-prefix detail** command shows the **recursive-via-host** and **recursive-via-connected** flags:

```
Router# show ip cef vrf vpn1 10.51.10.1 detail
```

```
10.51.10.1/24, epoch 0, flags rib defined all labels
  local label info: other/24
  recursive via 10.6.16.6 label 23
    nexthop 10.2.3.3 Ethernet1/0 label 17
  recursive via 10.1.2.1, repair
    attached
```

Table 47 describes the fields shown in the example.

Table 47 *show ip cef vrf Field Descriptions*

Field	Description
Prefix	Specifies the network prefix.
Next Hop	Specifies the Border Gateway Protocol (BGP) next hop address.
Interface	Specifies the VRF interface.

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.
show ip vrf	Displays VRF interfaces.

show ip cef with epoch

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

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

Syntax Description	<i>epoch-number</i>	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 FIB. This command is similar to the show ipv6 cef with epoch command, except that it is IPv4 specific. Use the show ip cef epoch command to display the epoch number.
-------------------------	---

Examples	The following is sample output from the show ip cef with epoch command:
-----------------	--

```
Router# show ip cef with epoch 0

Prefix          Next Hop          Interface
0.0.0.0/0       no route
0.0.0.0/8       drop
0.0.0.0/32      receive
10.1.1.1/32     receive          Loopback0
127.0.0.0/8     drop
224.0.0.0/4     drop
224.0.0.0/24    receive
240.0.0.0/4     drop
255.255.255.255/32 receive
```

Table 48 describes significant fields shown in the display.

Table 48 *show ip cef with epoch Field Descriptions*

Field	Description
Prefix	IP addresses in the FIB associated with the specified epoch.
Next Hop	What happens to the packet at the next hop.
Interface	Either the egress interface for the forwarded packet or the interface on which the packet is received.

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

```
Router# show ip cef with epoch 15 detail

IPv4 CEF is enabled and running
VRF Default:
  9 prefixes (9/0 fwd/non-fwd)
  Table id 0
  Database epoch:          0 (9 entries at this epoch)
```

Table 49 describes significant fields shown in the display.

Table 49 *show ip cef with epoch detail Field Descriptions*

Field	Description
IPv4 CEF is enabled and running	States whether Cisco Express Forwarding is enabled and running.
VRF Default	VRF table, in this instance, the default VRF.
9 prefixes ((9/0 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 (9 entries at this epoch)	Value of the database epoch and number of entries in the epoch.

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

```
Router# show ip cef with epoch 0 checksum

0.0.0.0/0
  FIB checksum: 0x353023B8
0.0.0.0/8
  FIB checksum: 0x6AAA2DEF
0.0.0.0/32
  FIB checksum: 0xC9136D79
10.1.1.1/32
  FIB checksum: 0x2DD79A12
127.0.0.0/8
  FIB checksum: 0x06E2709F
224.0.0.0/4
  FIB checksum: 0xC59D5F03
224.0.0.0/24
  FIB checksum: 0x9A64B149
240.0.0.0/4
  FIB checksum: 0x891B2D02
```

```
255.255.255.255/32
  FIB checksum: 0x72C832F4
```

Table 50 describes significant fields shown in the display.

Table 50 *show ip cef with epoch checksum Field Descriptions*

Field	Description
10.1.1.1/32	Prefix in epoch 0.
FIB checksum: 0x2DD79A12	FIB checksum associated with the named prefix.

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

```
Router# show ip cef with epoch 0 platform
```

```
0.0.0.0/0
0.0.0.0/8
0.0.0.0/32 receive
10.1.1.1/32 receive
127.0.0.0/8
224.0.0.0/4 multicast
224.0.0.0/24 multicast
240.0.0.0/4
255.255.255.255/32 receive
```

Table 51 describes significant fields shown in the display.

Table 51 *show ip cef with epoch platform Field Descriptions*

Field	Description
10.1.1.1/32 receive	Receive prefix in the specified database epoch.
224.0.0.0/4 multicast	Multicast address in the specified database epoch.

Related Commands

Command	Description
show ip cef	Displays entries in the FIB or displays a summary of the FIB.
show ip cef epoch	Displays epoch information for the adjacency table and all FIB tables.
show ipv6 cef with epoch	Displays Cisco Express Forwarding IPv6 FIB information filtered for a specific epoch.

show ip cef with source

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

```
show ip 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 FIB.
- **broadband**—Displays broadband receive prefix sources in the Cisco Express Forwarding FIB.
- **fallback**—Displays fallback lookup prefix sources in the Cisco Express Forwarding FIB.
- **interface**—Displays interface configuration prefix sources in the Cisco Express Forwarding FIB.
- **NAT**—Displays Network Address Translation (NAT) prefix sources in the Cisco Express Forwarding FIB.
- **rib**—Displays Routing Information Base (RIB) prefix sources in the Cisco Express Forwarding FIB.
- **special**—Displays special prefix sources in the Cisco Express Forwarding FIB.
- **test**—Displays test command prefix sources in the Cisco Express Forwarding FIB.
- **virtual**—Displays virtual address prefix sources in the Cisco Express Forwarding 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 releases:

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

Additional keywords for Cisco IOS Release 12.2(33)SXH and later SX releases only:

- **lte**—Displays Multiprotocol Label Switching (MPLS) label table entries.
- **recursive-resolution**—Displays recursive resolution prefix sources in the Cisco Express Forwarding FIB.

checksum	(Optional) Displays FIB entry checksums.
detail	(Optional) Displays detailed information about 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.
	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 a specified type of source prefix in the Cisco Express Forwarding FIB.

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

```
Router# show ip cef with source rib
```

```
Prefix           Next Hop          Interface
10.1.1.1/32      receive           Loopback0
```

Table 52 describes the significant fields shown in the display.

Table 52 *show ip cef with source rib Field Descriptions*

Field	Description
Prefix	List of prefixes in the Cisco Express Forwarding FIB whose source is the Routing Information Base (RIB).
Next Hop	Next-hop address, in general.
Interface	Either an egress interface or receive interface.

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

```
Router# show ip cef with source rib detail
```

```
IPv4 CEF is enabled and running
VRF Default:
  9 prefixes (9/0 fwd/non-fwd)
  Table id 0
  Database epoch:          0 (9 entries at this epoch)

10.1.1.1/32, epoch 0, flags attached, connected, receive
  Interface source: Loopback0
  receive for Loopback0
```

Table 53 describes the significant fields shown in the display.

Table 53 *show ip cef with source rib detail Field Descriptions*

Field	Description
VRF Default	Default VRF table.
9 prefixes (9/0 Fwd/non-fwd)	Number of prefixes in the VRF, how many of then are forwarded, and how many or not forwarded.
Table id 0	Table identification number.
Database epoch: 0 (9 entries at this epoch)	Number of the epoch (0) and number of entries in the epoch.
10.1.1.1/32, epoch 0, flags attached, connected, receive	Details about the prefix: the epoch in which it is found, and the flags that are set for the prefix: - attached—Prefix is connected to a network - connected—Prefix includes an address that is bound to an interface on the device - receive—Prefix is punted to and handled by the Process code rather than Cisco Express Forwarding
Interface source: Loopback0	Indicates that the source interface for the prefix was an interface, specifically Interface Loopback0.
receive for Loopback0	Indicates that the prefix is a receive type for the Lookback interface. Traffic matching this prefix will be punted to the process level and handled by the process code.

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 Cisco Express Forwarding FIB information filtered for a specific epoch.
show ipv6 cef with epoch	Displays Cisco Express Forwarding IPv6 FIB information filtered for a specific epoch.
show ipv6 cef with source	Displays Cisco Express Forwarding IPv6 FIB information filtered for a specific source.

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

<i>group-address</i>	(Optional) Address of the IP multicast group for which to display the MFIB table.
<i>source-address</i>	(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:

```

Table 54 describes the significant fields shown in the display.

Table 54 *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).
<i>vrf-name</i>	(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 <i>vrf-name</i> 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

Table 55 describes the significant fields shown in the display.

Table 55 *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
```

[Table 56](#) describes the fields in the display.

Table 56 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.

Table 56 *show ip mds stats switching Field Descriptions (continued)*

Field	Description
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
```

Table 57 describes the fields in the display.

Table 57 *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
hwindb stats      : 4775        swindb 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          mvrfl ext slotmask msg: 719
```

Table 58 describes the fields in the display.

Table 58 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.
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.

Table 58 *show ip mds stats ipc-msg switching Field Descriptions (continued)*

Field	Description
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.
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 MDIFS forwarding table erase messages received.
mdt mgid ext slotmask msg	Number of MDIFS MDT multicast global identifier (MGID) extended slotmask messages received.
mvrp ext slotmask msg	Number of MDIFS Multicast Virtual Routing and Forwarding (MVRP) extended slotmask messages received.

show ip mds summary

To display a summary of the Multicast Forwarding 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 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** 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
```


Table 59 describes the significant fields in the display.

Table 59 *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 <i>type</i> and <i>number</i> arguments. These modifications were made to provide support for the IPv4 MIBs as described in RFC 4293: <i>Management Information Base for the Internet Protocol (IP)</i> .

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
Frgs: 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

```

Cisco 10000 Series Routers Example

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

```

Table 60 describes the significant fields shown in the display.

Table 60 *show ip traffic Field Descriptions*

Field	Description
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.
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 Address Resolution Protocol (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 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.
<i>prefix</i>	(Optional) Entry prefix in the format A.B.C.D.
<i>mask-length</i>	(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.
<i>module number</i>	(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 <i>block-number</i>	(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 <i>reg-address</i>	(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.

Release	Modification
12.2(33)SXI	This command was modified. Support for the command was added for PCF3BXL, PFC3C, and PFC3CXL modes only.
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#
```

Table 61 describes the fields in the examples.

Table 61 *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. • <i>mac-address</i>—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 <i>ip-src-addr</i>	(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 <i>end-range</i>	(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.
<i>lower-flag</i>	Lower 32-bits flag values to display; valid values are 0 to FFFFFFFF.
<i>upper-flag</i>	Upper 32-bits flag values to display; valid values are 0 to FFFFFFFF.
mac-address <i>number</i>	(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.
<i>label</i>	(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 <i>number</i>	(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**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 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#
```

Supervisor Engine 2 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	Displays the numeric Virtual Private Network (VPN) routing and forwarding (VRF) ID for the specified VRF instance name.
<i>instance-name</i>	
<i>src-ip</i>	Source IP address.
<i>dest-ip</i>	Destination IP address.
<i>src-l4port</i>	Layer 4-source port number; valid values are from 0 to 65535.
<i>dest-l4port</i>	(Optional) Layer 4-destination port number; valid values are from 0 to 65535.
module <i>num</i>	(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 <i>instance-name</i> 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** *instance-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.

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.

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 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

Supervisor Engine 2 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#

Supervisor Engine 720 Example

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 <i>num</i>	(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 <i>num</i>	(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 section 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

<i>prefix</i>	(Optional) Entry prefix in the format A.B.C.D.
<i>mask-length</i>	(Optional) Mask length; valid values are from 0 to 32.
detail	(Optional) Displays hardware-entry details.
module <i>number</i>	(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 <i>prefix</i> 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

```
Router#
```

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
-----	-------------	-----------------	------

```
Router#
```

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    V130,          0050.808b.8200
81     200.1.1.91/32     V130,          0004.4eef.8800
82     200.1.1.100/32    V130,          00d0.bb02.0400
83     200.12.223.3/32   V130,          00d0.061b.7000
84     200.2.5.3/32      V130,          00d0.061d.200a
85     200.1.1.101/32    V130,          0007.ecfc.e40a
86     200.0.100.1/32    V130,          0050.2a8d.700a
87     200.1.1.104/32    V130,          0050.0f2d.ac00
88     223.255.254.226/32 V130,          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   V130,          0050.808b.8200
```

```

81      172.16.1.91/32      V130,      0004.4eef.8800
82      172.16.1.100/32     V130,      00d0.bb02.0400
83      172.17.223.3/32     V130,      00d0.061b.7000
84      172.22.5.3/32       V130,      00d0.061d.200a
85      172.16.1.101/32     V130,      0007.ecfc.e40a
86      172.20.100.1/32     V130,      0050.2a8d.700a
87      172.16.1.104/32     V130,      0050.0f2d.ac00
88      172.32.254.226/32   V130,      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#

```

Table 62 describes the fields shown in the examples.

Table 62 *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 <i>source-ip</i>	Displays hardware-entry information based on the specified source IP address.
detail	(Optional) Displays hardware-entry details.
group <i>group-id</i>	(Optional) Displays hardware-entry information that is based on the specified group IP address.
vlan <i>rpf-vlanid</i>	(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 <i>prefix</i>	(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 <i>src-ip</i>	(Optional) Displays the numeric Virtual Private Network (VPN) routing and forwarding (VRF) ID for the specified source IP address.
<i>src-port</i>	(Optional) Layer 4 source port; valid values are from 0 to 65535.

<i>dst-ip</i>	(Optional) Destination IP address.
<i>dst-port</i>	(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
* oifs]	226.2.2.0/24	Df0	BCp	0	0	-	V150 [1
* oifs]	225.2.2.0/24	Df1	BCp	0	0	-	V151 [1
* oifs]	227.2.2.0/24	Df1	BCp	0	0	-	V151 [1

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
  rwlans: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:000000000000 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
  rwlans: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:000000000000 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
  rwlans: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:000000000000 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
rwinde  Output V  lns/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
  rwlans:0 rwinde:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast l3rwld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0xA
  packets:000000000000 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
  rwlans:0 rwinde:0x0 adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
  fmt:mcast l3rwld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x8
  packets:000000000000 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
rwinde  Output V  lns/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   V151 [1 oifs]
*                227.2.2.0/24          -      Br     0          0
0x40E   V151 [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
  rwlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
  fmt:recir l3rwlvd: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
  rwlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
  fmt:mcast l3rwlvd: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
  rwlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
  fmt:mcast l3rwlvd: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
  rwlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
  fmt:recir l3rwlvd: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
  rwlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
  fmt:mcast l3rwlvd: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
  rwlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
  fmt:mcast l3rwlvd: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
  rwlans:0 rwindex:0x0 rdt:0 E:0 CAP1:0
  fmt:recir l3rwlvd: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:00000000000000 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:00000000000000 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     V151,V130 [2 oifs]
*          225.2.2.2/32          -      Br     0          0
0x40E     V151,V130 [2 oifs]
*          225.2.2.1/32          Df0    BCp    0          0          -
*          225.2.2.1/32          -      Bpr    0          0
0x4AE     V151,V130 [2 oifs]
*          225.2.2.1/32          -      Br     0          0
0x40E     V151,V130 [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:00000000000000 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:00000000000000 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
rwlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x22
packets:00000000000000 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
rwlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:0 E:0 CAP1:0
fmt:recir l3rwlvd:1 DM:0 mtu:1522 rwtype:RECIR
packets:00000000000000 bytes:000000000000000000

PI:1 (1) CR:0 (0) Recirc:1 (1)
AdjPtr:17,32785,65553,98321 FibRpfNf:0 FibRpfDf:0 FibAddr:0xE2
rwlans:0 rwindex:0x4AE adjmac:0006.d606.e240 rdt:1 E:1 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1E
packets:00000000000000 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
rwlans:0 rwindex:0x40E adjmac:0006.d606.e240 rdt:1 E:0 CAP1:0
fmt:mcast l3rwlvd:1 DM:0 mtu:1522 rwtype:L3 met2:0x0 met3:0x1E
packets:00000000000000 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.	
<i>vrf-name</i>	(Optional) VRF name.	
<i>ip-address/mask</i>	(Optional) Entry IPv6 address and prefix mask. Valid values for the <i>mask</i> 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.	
<i>src-addr</i>	Source IP address.	
<i>L4-src-port</i>	(Optional) Layer 4-source port number; valid values are from 0 to 65535.	
<i>dst-addr</i>	Destination IP address.	
<i>L4-dst-port</i>	(Optional) Layer 4-destination port number; valid values are from 0 to 65535.	
multicast tcam	Displays IPv6-multicast entries.	
<i>v6mcast-address</i>	(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: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:FFF:FFF:FFF:FFF:
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	<i>prefix</i>	(Optional) Entry prefix in the format A.B.C.D.
	<i>mask</i>	(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.

Defaults

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.
	<i>address</i>	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.
-------------------	--

Defaults

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.
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.

Defaults 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 examples of the **mls 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 <i>value</i>	(Optional) Displays the entries for a specific label; valid values are from 0 to 1048575.
	module <i>number</i>	(Optional) Displays the entries for a specific module.
	vpn <i>instance</i>	(Optional) Displays the Virtual Private Network (VPN) ID MPLS table entries for a specific VPN instance; valid values are from 0 to 4095.
	vrf <i>instance</i>	(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. <pre>Router# show mls cef statistics Total CEF switched packets: 0000000000000000 Total CEF switched bytes: 0000000000000000 Router#</pre>
-----------------	---

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	Supervisor Engine 720 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: <pre>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#</pre>
-----------------	---

Supervisor Engine 2 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#
```

12.2(33)SXI Example

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
```

[Table 63](#) describes the fields in the **show mls cef summary** command output.

Table 63 *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.
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	
<i>instance-name</i>	VPN routing/forwarding instance name; valid values are from 0 to 4095.
<i>prefix</i>	(Optional) Prefix of the entry to display.
detail	(Optional) Displays the hardware-entry details.
lookup <i>ip-address</i>	(Optional) Displays the longest prefix-match lookup entry for the specified address.
module <i>num</i>	(Optional) Displays the entries for a specific module.
rpf <i>ip-address</i>	(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 <i>number</i>	(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 Ear1
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 Ear1
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* | *hh:mm* } | **clock** *hh:mm* [*date month* | *month date*] | **from-boot** *seconds* | **latest** } | *component* { **all** | **back** { *mmm* | *hh:mm* } | **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 { <i>mmm</i> <i>hh:mm</i> }		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 (<i>mmm</i> or <i>hh:mm</i>).
clock <i>hh:mm</i>		Displays event trace messages starting from a specific clock time in hours and minutes format (<i>hh:mm</i>).
<i>date</i>	(Optional)	Day of the month.
<i>month</i>	(Optional)	Displays the month of the year.
from-boot <i>seconds</i>		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.
<i>component</i>	(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 command replaced the show cef events and show ip cef events commands.

Release	Modification
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 <i>component</i> 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 cfld keyword was added as an entry for the <i>component</i> 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 **cfld** 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

IPC Component Example

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
```

BFD Component for Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

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

```

SPA Component Example

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

```

Cisco Express Forwarding Component 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
```

Cisco Express Forwarding Component Examples for Cisco 10000 Series Routers Only

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
```

CFD Component for Cisco IOS Release 12.4(9)T

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 Assistance 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 cfn 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.
<i>trace-duration</i>	The time duration in hours and minutes format (mmm or hhh:mm).
clock <i>hh:mm</i>	Displays event trace messages starting from a specified time in hours and minutes format (hh:mm).
<i>date</i>	(Optional) Day of the month from 1 to 31.
<i>month</i>	(Optional) Month of the year.
from-boot	Displays event trace messages starting after booting up (uptime).
<i>seconds</i>	(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.
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.
<i>minutes</i>		Specifies the time argument in minutes. The time argument is specified in minutes format (mmm).
<i>hours:minutes</i>		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).
<i>day month</i>		(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.
<i>seconds</i>		(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.

[Table 64](#) describes the significant fields shown in the display.

Table 64 *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.
(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

```

Table 65 describes the significant fields shown in the display.

Table 65 *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 occurred.

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.
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.
<i>minutes</i>		Time argument (mmm) in minutes.
<i>hours:minutes</i>		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).
<i>day month</i>		(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.
<i>seconds</i>		(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
```

Table 66 describes the significant fields shown in the display.

Table 66 *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”.

Table 66 *show monitor event-trace cef events all Field Descriptions (continued)*

Field	Description
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.
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.
<i>minutes</i>		Time argument (mmm) in minutes.
<i>hours:minutes</i>		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).
<i>day month</i>		(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.
<i>seconds</i>		(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
<i>interface-index</i>		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.

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 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
.
.
.
```

Table 67 describes the significant fields shown in the display.

Table 67 *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	
<i>ip-address</i>	Specifies an IP address of interest in A.B.C.D format.
vrf <i>vrf-name</i>	Specifies a Cisco Express Forwarding IPv4 Virtual Private Network (VPN) routing and Forwarding (VRF) table. The <i>vrf-name</i> 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.
<i>minutes</i>	Time argument (mmm) in minutes.
<i>hours:minutes</i>	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).
<i>day month</i>	(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.
<i>seconds</i>	(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.

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 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]
.
.
.
```

[Table 68](#) describes the significant fields shown in the display.

Table 68 *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
```

Table 69 describes the significant fields shown in the display.

Table 69 *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.
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

<i>ipv6-address</i>	Specifies an IPv6 address. This address must be specified in hexadecimal values 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.
<i>minutes</i>	Time argument (mmm) in minutes.
<i>hours:minutes</i>	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).
<i>day month</i>	(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.
<i>seconds</i>	(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]
```

[Table 70](#) describes the significant fields shown in the display.

Table 70 *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.
[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
```

[Table 71](#) describes the significant fields shown in the display.

Table 71 *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.
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.
	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.
{ <i>mmm</i> <i>hhh:mm</i> }		Duration of the trace. The format is <i>mmm</i> or <i>hhh:mm</i> .
clock		Displays event trace messages starting from a specific clock time.
<i>hh:mm</i>		Integer value that is the length of time, in hours and minutes. The format is <i>hh:mm</i> .
<i>date</i>		(Optional) Day of the month (from 1 to 31).
<i>month</i>		(Optional) Displays the month of the year.
from-boot		Displays event trace messages starting from a specified number of seconds after booting.
<i>seconds</i>		(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.
<i>handle-number</i>		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)
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
  CPUs         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.
<i>time</i>		Duration of trace in the format mmm or hhh:mm.
clock		Displays trace from a specific clock time and date.
<i>time</i>		Time in the format hh:mm.
<i>day</i>		Day of the month.
<i>month</i>		Month of the year.
from-boot		Displays trace from specified seconds after booting.
<i>time</i>		(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.
	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	<i>trace-buffer-name</i>	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.

show pxf accounting

To show Parallel eXpress Forwarding (PXF) switching statistics for individual interfaces, use the **show pxf accounting** command in user EXEC or privileged EXEC mode.

show pxf accounting *interface* [*slot/port*]

Syntax Description

<i>interface</i>	Specifies the type of interface to display.
<i>slot</i>	(Optional) Backplane slot number. On the Cisco 7200 VXR series routers, the value can be from 0 to 6.
<i>port</i>	(Optional) Port number of the interface. On the Cisco 7200 VXR series routers, the value can be from 0 to 5.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)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.

Usage Guidelines

You can display information about the interface types shown in [Table 72](#) using the **show pxf accounting** command:

Table 72 *show pxf accounting Interface Types*

Keyword	Interface Type
atm	ATM interface
ethernet	Ethernet interface
fastethernet	FastEthernet interface
hssi	High Speed Serial interface
null	Null interface
pos	Packet-over-SONET interface
serial	Synchronous serial interface
summary	PXF summary statistics

Examples

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

```
Router# show pxf accounting ?

ATM          ATM interface
Ethernet     IEEE 802.3
FastEthernet FastEthernet IEEE 802.3
Hssi         High Speed Serial Interface
Null         Null interface
POS          Packet over Sonet
Serial       Serial
summary      PXF summary statistics
```

The following is sample output from the **show pxf accounting ethernet** command with an Ethernet interface in slot 4 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting ethernet 4/0
```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
Ethernet4/0	0	0	122	11490	4	0

The following is sample output from the **show pxf accounting null** command with a null interface in slot 0 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting null 0/0
```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
nu0/0	0	0	0	0	4932	0

The following is sample output from the **show pxf accounting pos** command with a Packet-over-SONET interface in slot 4 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting pos
```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
POS4/0	19	1064	0	0	44	0

The following is sample output from the **show pxf accounting serial** command with a serial interface in slot 5 on a Cisco 7200 VXR series router:

```
Router# show pxf accounting serial 5/0
```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
Serial5/0	0	0	0	0	0	0

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

```
Router# show pxf accounting summary
```

Pkts	Dropped	RP Processed	Ignored
Total	0	48360	0

PXF Statistic:
Packets RP -> PXF:

switch ip:	0
switch raw:	30048360
qos fastsend:	0
qos enqueue:	1938
Total:	30050298


```

Packets PXF -> RP:
  qos pkts:          1938
  fast pkts:        30000000
  drops:total        0
  punts:total        48360
  "    not IP      :    40572
  "    CEF no adjacency :    7788
Total:              30050298

Packets ignored:      0 | ring space:
  shadow ring full:    0 |   shadow ring:      16384
  in ring full:        0 |   inring:           968
  PXF inactive:        0

tx credits:           16230330 | delayed credits:      0
holdq enqueues:        0 | requeue drops:        0
interrupts:            40538 | interrupt misses:     1947
interrupt packets:     53326
pending read bytes:    0

```

Interface	Pkts In	Chars In	Pkts Out	Chars Out	Punted	Dropped
Fa0/0	0	0	30000000	1740000000	970	0
Et1/0	0	0	0	0	21309	0
Et1/1	0	0	0	0	0	0
Et1/2	0	0	0	0	0	0
Et1/3	0	0	0	0	0	0
Se2/0	0	0	0	0	963	0
Se2/1	0	0	0	0	0	0
Se2/2	0	0	0	0	0	0
Se2/3	0	0	0	0	0	0
Fa3/0	0	0	0	0	963	0
PO4/0	30000000	1440000000	0	0	963	0
AT5/0	0	0	0	0	23192	0
Vi1	0	0	0	0	0	0
Vt1	0	0	0	0	0	0
Vi2	0	0	0	0	0	0

Related Commands

Command	Description
show pxf crash	Displays PXF crash information.
show pxf feature	Displays the PXF routing feature tables for enabled PXF features.
show pxf interface	Displays a summary of the interfaces in the router and the PXF features or capabilities enabled on these interfaces.

show pxf cpu access-lists

To display Parallel eXpress Forwarding (PXF) memory information for access control lists (ACLs), use the **show pxf cpu access-lists** command in privileged EXEC mode.

show pxf cpu access-lists [**security** | **qos** | **pbr** | **compiled**]

Cisco 10000 Series Router

show pxf cpu access-lists [**security** [[**tcam** *acl-name* [**detail**]] | **flex-sum** | **children**] | **qos** | **pbr** | **compiled**]

Syntax Description	
security	(Optional) Displays information about the security ACLs defined in Cisco IOS and compiled to the PXF. Also displays information about split ACLs, such as how much memory has been used.
tcam <i>acl-name</i>	(Optional) Displays information about the specified security ACL stored in ternary content addressable memory (TCAM). This option is only available on the PRE3 for the Cisco 10000 series router.
detail	(Optional) Displays decoded information about the packet fields used for matching in the TCAM.
flex-sum	(Optional) Displays summary information describing the amount of memory allocated in the parallel express forwarding (PXF) engine for use by the flexible key construction microcode. This information is useful for design teams. This option is only available on the PRE3 for the Cisco 10000 series router.
children	(Optional) Displays information for child policies. If an ACL is a template child, the output typically does not display the child information. Specifying the children keyword displays data for child policies, too, and shows the children and the parent policy of each child. Use caution when using the children keyword as there might be thousands of child policies configured, which could have negative effects on the command output.
qos	(Optional) Displays information about the QoS ACLs defined in Cisco IOS and compiled to the PXF.
pbr	(Optional) Displays information about ACLs for policy-based routing (PBR).
compiled	(Optional) Displays information for all compiled Turbo-ACLs. The PRE2 supports Turbo-ACLs and the compiled option. The PRE3 accepts the PRE2 compiled option, but does not implement Turbo-ACLs.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.3(7)XI1	This command was introduced on the PRE2 for the Cisco 10000 series router.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Usage Guidelines**Cisco 10000 Series Router (PRE2)**

Because memory is shared between TurboACLs and MiniACLs, they can interfere with each other's capacities. The Mini-ACL is automatically set up with space for 8191 Mini-ACLs at router start. If more than 8191 Mini-ACLs are created, another block of MiniACLs (4096) is allocated. This process is repeated as necessary until the router is out of External Column Memory (XCM) in any one bank that the Mini-ACLs need.

Cisco 10000 Series router (PRE3)

The PRE3 implements only TCAM ACLs. Turbo-ACLs and Mini-ACLs are not supported.

Examples

The sample output from the **show pxf cpu access-lists security** command (see [Sample Output](#)) is based on the configuration of the access control list (ACL) called test_list (see [ACL Configuration](#)). The sample output is divided into several sections with a description of the type of information displayed in each.

ACL Configuration

```
Router# show pxf cpu access-lists test_list
```

```
Extended IP access list test_list (Compiled)
```

```
10 permit ip any host 10.1.1.1
20 permit ip any host 10.1.1.2
30 permit ip any host 10.1.1.3
40 permit ip any host 10.1.1.4
50 permit ip any host 10.1.1.5
60 permit ip any host 10.1.1.6
70 permit ip any host 10.1.1.7
80 permit ip any host 10.1.1.8
90 permit ip any host 10.1.1.9
100 permit ip any host 10.1.1.11
110 permit ip any host 10.1.1.12
```

Sample Output

The following sample output describes the information displayed in the first section of the command output from the **show pxf cpu access-lists security** command:

```
Router# show pxf cpu access-lists security
```

```
PIX Security ACL statistics:
```

ACL	State	Tables	Entries	Config	Fragment	Redundant	Memory	ACL_index
1	Operational	1	-	-	-	-	0Kb	1
sl_def_acl	Operational	2	-	-	-	-	0Kb	2
test	Operational	3	-	-	-	-	0Kb	3
test_list	Operational	1	12	11	0	0	7Kb	1

Table 73, Part 1, describes the significant fields shown in the display.

Table 73, Part 1 *show pxf cpu access-lists security Field Descriptions*

Field	Description
ACL	Identifies the ACL by name or number.
State	Displays the current state of the ACL: - Copying—ACL is in the process of being created or compiled. - Operational—ACL is active and filtering packets. - Out of acl private mem—ACL has run out of the private memory that was allocated exclusively to it. - Out of shared mem—ACL has run out of the memory that it shares with other ACLs. - Unknown Failure—ACL has failed because of an uncategorized reason. - Unneeded—ACL was allocated but is not currently in use.
Tables	An indicator of whether the ACL has been split into more than one PXF pass. The first three ACLs in the output are MiniACLs, and have the ACL_index duplicated in the Tables column.
Entries	The count of ACL rules as seen by the Turbo compiler. This is the sum of the Config, Fragment, and Redundant columns plus 1.
Config	The count of rules for this ACL.
Fragment	The count of extra rules added to handle fragment handling, where Layer 4 information is needed but not available in a packet fragment.
Redundant	The count of rules that are not needed because they are covered by earlier rules.
Memory	The amount of PXF XCM in use for the ACL.
ACL_index	The index of the ACL in XCM.

The following sample output describes the information displayed in the next section of the command output from the **show pxf cpu access-lists security** command:

First level lookup tables:

Block	Use	Rows	Columns	Memory used
0	TOS/Protocol	1/128	1/32	16384
1	IP Source (MS)	1/128	1/32	16384
2	IP Source (LS)	1/128	1/32	16384
3	IP Dest (MS)	2/128	1/32	16384
4	IP Dest (LS)	12/128	1/32	16384
5	TCP/UDP Src Port	1/128	1/32	16384
6	TCP/UDP Dest Port	1/128	1/32	16384
7	TCP Flags/Fragment	1/128	1/32	16384

Table 73, Part 2, describes the significant fields shown in the display.

Table 73, Part 2 *show pxf cpu access-lists security Field Descriptions*

Field	Description
Block	Indicates the block number.
Use	Describes the IP packet field that is being matched.
Rows	An indication of where the largest variety of values are in use in the ACLs that are being applied. In the output, 12/128 means that there are 12 different values of significance in the field. If there are other rules added and the value exceeds 128, more memory will be needed to accommodate the new rules.
Columns	An indication of the number of TurboACLs in PXF memory. In the output, 1/32 means there is only one TurboACL in PXF memory. If there are more than 31 added, another chunk of memory is needed to accommodate the new ACLs.
Memory used	Displays the total amount of memory used for this particular lookup table.

The following sample output describes the information displayed in the next section of the command output from the **show pxf cpu access-lists security** command. There are 16 banks of XCM in each PXF column. This output section shows the usage level of each bank.

Banknum	Heapsize	Freesize	%Free
0	4718592	4702208	99
1	8126464	6012928	73
2	8388608	6290432	74
3	8388608	6290432	74
4	5898240	5881856	99
5	8126464	6012928	73
6	8388608	6290432	74
7	8126464	6012928	73
8	4456448	4440064	99
9	8126464	6012928	73

Table 73, Part 3, describes the significant fields shown in the display.

Table 73, Part 3 *show pxf cpu access-lists security Field Descriptions*

Field	Description
Banknum	The block of memory used for this particular lookup table.
Heapsize	The total amount of memory, in bytes, allocated for this block.
Freesize	The amount of memory, in bytes, that is currently available for use by this block of memory.
%Free	The percentage of memory that is free and available for use for this block of memory. When the %Free drops to 0, the router cannot hold any more ACLs in PXF memory, and any new ACL will not pass traffic.

This section of the sample command output indicates the memory usage of the MiniACLs in the router. All of the rows state about the same thing. To determine the actual number of MiniACLs in play, divide the memory used in any of blocks 1 to 10 by 256, or blocks 11 to 14 by 16.

MiniACL XCM Tables:

Block	Use	Memory Used	%Free
0	IP Src 1	768	99
1	IP Src 2	768	99
2	IP Src 3	768	99
3	IP Src 4	768	99
4	IP Dest 1	768	99
5	IP Dest 2	768	99
6	IP Dest 3	768	99
7	IP Dest 4	768	99
8	ToS	768	99
9	Protocol	768	99
10	TCP Flags/Fragment	768	99
11	Source Port 1	48	99
12	Source Port 2	48	99
13	Destination Port 2	48	99
14	Destination Port 2	48	99

The following describes the information displayed in the last section of the sample output from the **show pxf cpu access-lists security** command:

```
Available MiniACL count = 8191
Usable ranges(inclusive):
1->8191
```

Table 73, Part 4, describes the significant fields shown in the display.

Table 73, Part 4 *show pxf cpu access-lists security Field Descriptions*

Field	Description
Available MiniACL	The number of ACLs currently available for allocation in XCM.
Usable ranges	The ACL indexes that will be assigned to MiniACLs.

PRE2 and PRE3 Security ACLs Examples (Cisco 10000 Series Router)

This section compares the output from the **show pxf cpu access-lists security** command when issued on the PRE2 and PRE3.

For the PRE2, the following sample output displays VMR (value, plus a mask and result) data for the ACL named ICMP_IGMP_MATCH:

```
Router# show pxf cpu access-lists security tcam ICMP_IGMP_MATCH detail
```

```
-----
VMR Format - handle: 524607B4
Format has 5 fields, refcount = 1
Field: Format, FIXED, start_bit = 69, end_bit = 71
Field: ACL index, FIXED, start_bit = 54, end_bit = 68
Field: Flags, FIXED, start_bit = 43, end_bit = 53
Field: L4 proto, FIXED CNV, start_bit = 16, end_bit = 23
Field: L4 source port, FIXED CNV, start_bit = 0, end_bit = 15 Total bits = 53, format = 72
GMR used: 5 Col 2 LKBP Vector: 544
-----
VMRs
----- VMR 0 -----
```

```

V: 001B0000 0000010B 00
M: FFFFC000 0000FFFF FF
R: 00010001
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00000B00/0000FFFF
L4 proto: 00000001/000000FF
Flags: 00000000/00000000
----- VMR 1 -----
V: 001B0000 00000103 01
M: FFFFC000 0000FFFF FF
R: 00010002
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00000301/0000FFFF
L4 proto: 00000001/000000FF
Flags: 00000000/00000000
----- VMR 2 -----
V: 001B0000 00000213 00
M: FFFFC000 0000FFFF 00
R: 00010003
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00001300/0000FF00
L4 proto: 00000002/000000FF
Flags: 00000000/00000000
----- VMR 3 -----
V: 001B0000 00000214 00
M: FFFFC000 0000FFFF 00
R: 00010004
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00001400/0000FF00
L4 proto: 00000002/000000FF
Flags: 00000000/00000000

```

For the PRE3, the following sample output displays for the **show pxf cpu access-lists security** command. Notice that the output does not include the columns shown above that are relevant to only the PRE2 and the output no longer displays first-level lookup tables.

Router# **show pxf cpu access-lists security**

```

PXF Security ACL statistics:
ACL                               State          ACL_index
STANDARD_MATCH_PERMIT           Operational    116
SRC_IP_MATCH144                 Operational    102
DST_IP_MATCH                    Operational    113
DST_IP_MATCH144                 Operational    112
PROTOCOL_MATCH                  Operational    104
PROTOCOL_MATCH144               Operational    103
FRAG_MATCH                      Operational    109
PRECEDENCE_TOS_MATCH            Operational    106
PRECEDENCE_TOS_MATCH144         Operational    105

```

Related Commands

Command	Description
show pxf cpu statistics	Displays PXF CPU statistics.
show pxf statistics	Displays a chassis-wide summary of PXF statistics.

show pxf cpu atom

To display Parallel eXpress Forwarding (PXF) CPU Any Transport over MPLS (AToM) forwarding information for an interface or Virtually Cool Common Index (VCCI), use the **show pxf cpu atom** command in privileged EXEC mode.

show pxf cpu atom [*interface-name* | *vcci*]

Syntax Description

<i>interface-name</i>	(Optional) Name of the interface.
<i>vcci</i>	(Optional) VCCI entry identifier.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB	This command was introduced on the Cisco 10000 series router.

Examples

The following example shows AToM forwarding information for Gigabit Ethernet interface 6/0/0. The fields shown in the display are self-explanatory.

Router#: **show pxf cpu atom gigabitethernet 6/0/0**

```
Imposition Information for VCCI 0x9E2:
  Output VCCI: 0x0
  Mac rewrite index: 0x0 extension: 0x0
  Ingress Flags: 0x0
  PTI Action Table: 0x0
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information about AToM VCs that are enabled to route Layer 2 packets on a router.
show pxf cpu mpls	Displays PXF MPLS FIB entry information.
show pxf cpu subblocks	Displays subblocks information that includes column 0 of AToM.

show pxf cpu bba

To display information on Parallel eXpress Forwarding (PXF) CPU Broadband Aggregation (BBA) groups, use the **show pxf cpu bba** command in privileged EXEC mode.

show pxf cpu bba

Syntax Description	This command has no arguments or keywords.
---------------------------	--

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

Command History	Release	Modification
	12.2S	This command was introduced.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples	The following example shows BBA groups information in the PXF CPU:
-----------------	--

Router# **show pxf cpu bba**

```
6w3d: show_pxf_bba
6w3d: %IPCOIR-4-REPEATMSG: IPC handle already exists for 1/0
6w3d: %IPCOIR-2-CARD_UP_DOWN: Card in slot 1/0 is down. Notifying 4oc3atm-1 dr.
6w3d: %C10K_ALARM-6-INFO: ASSERT CRITICAL slot 1 Card Stopped Responding OIR Al
6w3d: %IPCOIR-5-CARD_DETECTED: Card type 4oc3atm-1 (0x2D8) in slot 1/0
6w3d: %IPCOIR-5-CARD_LOADING: Loading card in slot 1/0 sw version 1.1 code MD5 C
6w3d: %C10K-5-LC_NOTICE: Slot[1/0] 4oc3atm-1 Image Downloaded...Booting...
6w3d: %IPCOIR-5-CARD_DETECTED: Card type 4oc3atm-1 (0x2D8) in slot 1/0
6w3d: %C10K_ALARM-6-INFO: CLEAR CRITICAL slot 1 Card Stopped Responding OIR Ala
6w3d: %IPCOIR-2-CARD_UP_DOWN: Card in slot 1/0 is up. Notifying 4oc3atm-1 driv.
```

Related Commands	Command	Description
	bba-group pppoe	Configures a BBA group to establish PPPoE sessions.

show pxf cpu buffers

To display packet buffer memory for temporary packet storage in the Cisco Internetwork Performance Monitor (IPM) of the Parallel eXpress Forwarding (PXF), use the **show pxf cpu buffers** command in privileged EXEC mode.

show pxf cpu buffers

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced on the Cisco 10000 series router.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines This command provides information about the number of handles that are used and available. Handles are outstanding packets in the virtual time management system (VTMS).

Examples The following example shows the number of handles that are used and available:

```
Router# show pxf cpu buffers

Cobalt2 ttc running.
Calculations could be off by (+/-) cache sizes.
      cache size
small   512
large   128

pool    # handles   available
-----
small   524288      523808
large   32768       32624
```

Table 74 describes the fields shown in the display.

Table 74 show pxf cpu buffers Field Descriptions

Field	Description
pool	Identifies the buffer pool.
# handles	The number of handles that are currently used.
available	The number of handles that are currently available.

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf cpu cef

The **show pxf cpu cef** command is replaced by the **show ip cef platform** command on the Cisco 10000 series router. See the **show ip cef platform** command for more information.

show pxf cpu context

To display the current and historical loads on the Parallel eXpress Forwarding (PXF), use the **show pxf cpu context** command in privileged EXEC mode.

show pxf cpu context

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced on the Cisco 10000 series router.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples

The **show pxf cpu context** command shows how busy the PXF forwarding process (FP) is with the current traffic load. The first section displays the number of contexts of each type that have entered the PXF engine since it was last reloaded. If counters are idle, the PXF pipeline is not operating properly.

Router# **show pxf cpu context**

```

FP context statistics      count      rate (since last time command was run)
-----
  feed_back               168635      0
  new_work_from_lc        7474477     13
  new_work_from_rp        964679      1
  new_work_from_replay    0           0
  null_context            3797097495884 6312156
-----
                              6312170
FP average context/sec    1min      5min      60min
-----
  feed_back               0          0          0      cps
  new_work_from_lc        8          8          8      cps
  new_work                 1          1          1      cps
  new_work_from_replay    0          0          0      cps
  null_context            6312260    6312261    6312250    cps
-----
  Total                   6312270    6312271    6312260    cps

FP context utilization    1min      5min      60min
-----
  Actual                  0 %       0 %       0 %
  Theoretical              0 %       0 %       0 %
  Maximum                 98 %      98 %      98 %

```

Table 74 describes the significant fields shown in the display.

Table 75 *show pxf cpu context Field Descriptions*

Field	Description
FP context statistics	
feed_back	Packets requiring additional passes through the pipeline. This counter is incremented once for each additional pass.
new_work	New packets input to the PXF pipeline. This counter represents a snapshot of the amount of incoming traffic being processed by the processor.
null_context	An indication of unused forwarding bandwidth (idle time). This counter is incremented for every context during which the PXF pipeline is not processing traffic. This counter represents the processor's potential to handle additional traffic. As the processor becomes more busy, the value for null decreases until it becomes zero, at which point the processor has reached its maximum usage.
FP average context/sec	
feed_back	Displays the rate, in terms of the number of contexts per second (cps) for the feed_back counter for the last 1-minute, 5-minute, and 60-minute time periods.
new_work	Displays the rate, in terms of the number of contexts per second (cps) for the new_work counter for the last 1-minute, 5-minute, and 60-minute time periods.
null_context	Displays the rate, in terms of the number of contexts per second (cps) for the null_counter for the last 1-minute, 5-minute, and 60-minute time periods.
FP context utilization	
Actual	Displays the actual percentage of processor usage per second, compared to the theoretical maximum, for the last 1-minute, 5-minute, and 60-minute time periods.
Theoretical	Displays the percentage of processor usage compared to the ideal theoretical capacities for the last 1-minute, 5-minute, and 60-minute time periods. The theoretical maximum for the PXF processors is 3,125,000 contexts per second (cps).
Maximum	Displays the actual maximum percentage of processor usage that has occurred for the last 1-minute, 5-minute, and 60-minute time periods.

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf cpu feedback

To display the total number of feedbacks through the Parallel eXpress Forwarding (PXF) by all packets, use the **show pxf cpu feedback** command in privileged EXEC mode.

show pxf cpu feedback

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced on the Cisco 10000 series router.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples The following example shows feedback counters information:

Router# **show pxf cpu feedback**

Load for five secs: 5%/0%; one minute: 6%; five minutes: 2%
Time source is hardware calendar, *21:13:02.615 UTC Tue Nov 29 2005

FP column 0 feedback counts

Global packet handle retry counter = 0

Name	Current	Difference (since last show)
-----	-----	-----
bypass	= 0	0
schedule retry	= 0	0
WRED sample	= 0	0
MLPPP linkq update	= 0	0
IP frag	= 0	0
ICMP	= 0	0
layer2 divert	= 0	0
tunnel lookup	= 0	0
tunnel RX	= 0	0
tunnel TX	= 0	0
output qos	= 0	0
tag not ip	= 0	0
netflow accumulate	= 0	0
netflow age	= 0	0
netflow swap	= 0	0
netflow export	= 0	0
PBR	= 0	0
input secACL log	= 0	0
input secACL split	= 0	0
output secACL log	= 0	0
output secACL split	= 0	0
IPC response	= 0	0
IPC MLPPP flush	= 0	0
input qos split	= 0	0

```

output qos split           = 0          0
MLPPP fwd packet          = 0          0
MLPPP background          = 0          0
MLPPP flush                = 0          0
drop                      = 0          0
QPPB                      = 0          0
mcast lookup              = 0          0
mcast replicate           = 0          0
mcast rpf failed          = 0          0
mcast bypass              = 0          0
PBR split                 = 0          0
MLPPP lock retry          = 0          0
output secACL             = 0          0
qos divert split          = 0          0
qos inject split          = 0          0
secACL divert split       = 0          0
MLPPP frag                = 0          0
mpls deaggregation        = 0          0
tunnel in secACL log      = 0          0
tunnel out secACL log     = 0          0
no packet handle          = 0          0
PBR to FIB                = 0          0
MLPPP flush lock retry    = 0          0
MLPPP flush setup         = 0          0
MLPPP sync flush req      = 0          0
tail drop IP frag         = 0          0
RP inject                 = 0          0
feedback retry            = 0          0
MLPPP discard feedback    = 0          0
MLPPP stats copy IPC      = 0          0
IPM replay                = 0          0
IPM replay drop           = 0          0
IP reasm lock retry       = 0          0
IP reasm recover punt     = 0          0
IP reasm forward          = 0          0
IP reasm insertion        = 0          0
LAC switch                = 0          0
L2TP decap                = 0          0
IP reasm fb divert qos    = 0          0
keepalive                 = 0          0
drop stats redirect       = 0          0
AToM multiplexed          = 0          0
LFI reassembly            = 0          0
LFI remove entry          = 0          0
iEdge translation         = 0          0
iEdge divert              = 0          0
multiple input qos        = 0          0
multiple output qos       = 0          0
iEdge PBHK DS trans       = 0          0
LAC switch qos            = 0          0
WRED sample init          = 0          0
replay egress             = 0          0
IPV6 FIB                  = 0          0
ICMPV6                    = 0          0
IPV6 ACL                  = 0          0
IPV6 DIVERT ACL           = 0          0
Total                     = 0          0

```

Related Commands**Command****Description**

show pxf cpu context Displays the current and historical loads on the PXF.

show pxf cpu iedge

To display Parallel eXpress Forwarding (PXF) policy and template information, use the **show pxf cpu iedge** command in privileged EXEC mode.

show pxf cpu iedge [**detail** | **policy** *policy-name* | **template**]

Syntax Description	detail	(Optional) Displays detailed information about policies and templates.
	policy <i>policy-name</i>	(Optional) Displays summary policy information.
	template	(Optional) Displays summary template information.

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

Command History	Release	Modification
	12.2S	This command was introduced.

Examples The following example shows PXF template information. The fields shown in the display are self-explanatory.

Router# **show pxf cpu iedge template**

```

Super ACL name           OrigCRC   Class Count   CalcCRC
1sacl_2                  4EA94046    2             00000000
if_info 71BA3F20

```

Related Commands	Command	Description
	show pxf statistics	Displays a summary of PXF statistics.

show pxf cpu ipv6

To display Parallel eXpress Forwarding (PXF) IPv6 statistics, use the **show pxf cpu ipv6** command in privileged EXEC mode.

```
show pxf cpu ipv6 [ipv6: address [prefix] | acl-prefixes | hash | summary]
```

Cisco 10000 Series Router

```
show pxf cpu ipv6 [acl-prefixes | address | hash | summary | table | vrf]
```

Syntax Description

<i>ipv6: address [prefix]</i>	(Optional) Specifies the IPv6 address and optional IPv6 prefix for the information you want to display.
acl-prefixes	(Optional) Displays access control list (ACL) prefixes mapping information.
address	(Optional) Displays PXF IPv6 address-specific information.
hash	(Optional) Displays hash table summary information.
summary	(Optional) Displays a summary of the PXF IPv6 statistics.
table	(Optional) Displays detailed information about the PXF IPv6 forwarding table.
vrf	(Optional) Displays PXF IPv6 VRF information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command was enhanced to provide the address , table , and vrf options, and implemented on the Cisco 10000 series router for the PRE3 and PRE4.

Usage Guidelines

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the **show pxf cpu ipv6 table** command displays the global table, but does not display the leafs that correspond to the IPv6 prefixes ::1/128 (Loopback) and ::/128 (All Zero). The microcode checks for these prefixes.

The **show pxf cpu ipv6 table** command replaces the **show pxf cpu ipv6** command in Cisco IOS Release 12.2(31)SB.

Examples

The following example shows the PXF IPv6 statistics:

```
Router# show pxf cpu ipv6

Mtrie Leaf Data: Prefix/Length

Leaf prefix ::/0,ACL Index = 0
```

```

Leaf elt_addr: 0x70D20001 SW_OBJ_FIB_ENTRY: 0x20A6E404 acl_index: 0
Refcount: 514 Flags: 0x2 Parent: None
First Covered: None
Right Peer: None
=====
0 routes in Mtrie with less specific overlapping parent route

```

Hash Table Leaf Data: Prefix/Length

```

Leaf prefix ::1/128,ACL Index = 0
Leaf elt_addr: 0x70D20011 SW_OBJ_FIB_ENTRY: 0x0 acl_index: 0
128-bit Table Hash Value: 0xC7F7
Refcount: 3 Flags: 0x2 Parent: None
First Covered: None
Right Peer: None
Leaf prefix ::1/128,ACL Index = 0
Leaf elt_addr: 0x70D20009 SW_OBJ_FIB_ENTRY: 0x0 acl_index: 0
128-bit Table Hash Value: 0xC2719
Refcount: 3 Flags: 0x2 Parent: None
First Covered: None
Right Peer: None
=====
0 routes in Hash Table with less specific overlapping parent route

```

Related Commands

Command	Description
show pxf cpu statistics	Displays PXF CPU statistics.

show pxf cpu mpls

To display Parallel eXpress Forwarding (PXF) Multiprotocol Label Switching (MPLS) Forwarding Information Base (FIB) information, use the **show pxf cpu mpls** command in privileged EXEC mode.

show pxf cpu mpls [**labels** *label-value* | **vrf**]

Syntax Description	labels <i>label-value</i>	(Optional) Displays the transport type and output features associated with the specified label value or label range. The <i>label-value</i> range is 0 to 524288.
	vrf	(Optional) Displays virtual routing and forwarding (VRF) root information.

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

Command History	Release	Modification
	12.2S	This command was introduced.

Examples

The following example shows VRF root information. The fields shown in the display are self-explanatory.

```
Router# show pxf cpu mpls vrf
VRF_ID 0      FIB_ROOT(RP) 0x72400000
```

Related Commands	Command	Description
	ping mpls	Checks MPLS LSP connectivity.
	show mpls interfaces	Displays information about the interfaces configured for label switching.
	show pxf cpu statistics	Displays PXF CPU statistics.
	trace mpls	Discovers MPLS LSP routes that packets will take when traveling to their destinations.

show pxf cpu mroute

To display Parallel eXpress Forwarding (PXF) multicast route (mroute) information, use the **show pxf cpu mroute** command in privileged EXEC mode.

show pxf cpu mroute [*ipaddress1*] [*ipaddress2*]

Syntax Description	[<i>ipaddress1</i>] [<i>ipaddress2</i>]	(Optional) Displays PXF mroute information for a particular group or range of groups.
--------------------	--	---

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

Command History	Release	Modification
	12.2S	This command was introduced.

Examples

The following example shows PXF mroute information:

Router# **show pxf cpu mroute**

Shadow G/SG[5624]: s: 0.0.0.0 g: 224.0.1.40 uses: 0 bytes 0 flags: [D] LNJ

Interface	vcci	offset	rw_index	mac_header
-----------	------	--------	----------	------------

In :	0	0x000004		
------	---	----------	--	--

Shadow G/SG[3195]: s: 0.0.0.0 g: 234.5.6.7 uses: 0 bytes 0 flags: [5] NJ

Interface	vcci	offset	rw_index	mac_header
-----------	------	--------	----------	------------

In :	0	0x000008		
------	---	----------	--	--

Out: Cable5/1/0	5	0x00002C	1B	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable6/1/1	9	0x000028	1A	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable6/0/0	6	0x000024	19	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable5/0/0	3	0x000020	18	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable7/0/0	A	0x00001C	17	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable7/1/1	C	0x000018	16	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable7/1/0	B	0x000014	15	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable6/1/0	8	0x000010	14	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable6/0/1	7	0x00000C	13	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Out: Cable5/0/1	4	0x000008	12	00000026800001005E05060700010
-----------------	---	----------	----	-------------------------------

Table 76 describes the fields shown in the display.

Table 76 *show pxf cpu mroute Field Descriptions*

Field	Description
Interface	Interface or subinterface.
vcci	Virtually Cool Common Index (VCCI) for the interface or subinterface.
rw index	Index used to read and write into the multicast table for this entry.
mac_header	MAC header that is used when rewriting the packet for output.

Related Commands

Command	Description
show ip mroute	Displays the Cisco IOS version of a multicast routing table entry.
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf cpu pbr action

To display policy-based routing (PBR) actions configured in the Parallel eXpress Forwarding (PXF), use the **show pxf cpu pbr action** command in privileged EXEC mode.

show pxf cpu pbr action *map-name*

Cisco 10000 Series Router (PRE3)

show pxf cpu pbr [**action** *map-name* | **tcam** *map-name* | **flex-sum**]

Syntax Description		
action <i>map-name</i>	(Optional) Displays PBR action information and redirects the command output to the route map you specify.	
tcam <i>map-name</i>	(Optional) Displays VMR (value, plus a mask and result) information stored in ternary content addressable memory (TCAM) and redirects the command output to the route map you specify.	
	Note This option is only available on the PRE3 for the Cisco 10000 series router.	
flex-sum	(Optional) Displays summary information describing the amount of memory allocated in the PXF engine for use by the flexible key construction microcode. This information is useful for design teams.	
	Note This option is only available on the PRE3 for the Cisco 10000 series router.	

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI1	This command was introduced on the Cisco 10000 series router for the PRE2.
	12.2(31)SB2	This command was introduced on the Cisco 10000 series router for the PRE3.

Usage Guidelines This command is useful to determine if an adjacency has been found for a **set ip next-hop ip-address** route map configuration command.

Examples

The following example shows the PBR route maps configured in the PXF:

```
Router# show pxf cpu pbr action foo
```

```
Show PBR Action:
```

```
-----
Policy number: 1
route-map foo, permit, sequence 10
  map number      = 0
  action index    = 0
    primary action : SET_ROUTE
    secondary action : - none -
  mac-rewr index = 0x0000 0015
  vcci = 0x09D4, qos group = 0, tos prec = 0
  tt_pkt_count = 0          tt_byte_count = 0
Adjacency data 0x20D29968
XCM adjacency from 0x70000120(RP)
0xA0000120(FP) index 0x24:
```

Cisco 10000 Series Router (PRE3)

The following configuration example shows a PBR configuration in which traffic classification is based on the IP access list named `pbr_length`. The route map permits traffic based on the specified matching criteria and sets the next hop address of each packet.

```
ip access-list extended pbr_length
  permit tcp any any
!
route-map pbr_length permit 10
  match ip address pbr_length
  match length 100 200
  set ip next-hop 2.0.95.5          !
route-map pbr_length permit 20
  match ip address pbr_length
  match length 200 300
  set ip next-hop 2.0.95.5          !
route-map pbr_length permit 30
  match length 300 400
  set ip next-hop 2.0.95.5          !
```

The following sample output from the `show pxf cpu pbr` command shows the type of information that displays based on the above PBR configuration:

```
Router# show pxf cpu pbr action pbr_length
```

```
Show PBR Action:
```

```
-----
Policy number: 3

route-map pbr_length, permit, sequence 10
  map number      = 0
  action index    = 64
  map vcci out    = 0x0
  tt_pkt_count    = 0          tt_byte_count = 0

  primary action  : NULL_ACTION
  secondary action : - none -
  mac-rewr index = 0x0000 0000
  vcci = 0x0000, qos group = 0, tos prec = 0
.....

route-map pbr_length, permit, sequence 20
```



```

map number      = 1
action index    = 65
map vcci out    = 0x0
tt_pkt_count    = 0                tt_byte_count = 0

primary action   : NULL_ACTION
secondary action : - none -
mac-rewr index  = 0x0000 0000
vcci = 0x0000, qos group = 0, tos prec = 0

.....

route-map pbr_length, permit, sequence 30
map number      = 2
action index    = 66
map vcci out    = 0x0
tt_pkt_count    = 0                tt_byte_count = 0

primary action   : NULL_ACTION
secondary action : - none -
mac-rewr index  = 0x0000 0000
vcci = 0x0000, qos group = 0, tos prec = 0

```

The following sample output from the **show pxf cpu pbr tcam** command shows the type of detailed VMR (value, plus a mask and result) information that displays:

Router# **show pxf cpu pbr tcam pbr_length detail**

VMR data for Route-map pbr_length

```

-----
VMR Format - handle: 5050BC90
Format has 5 fields, refcount = 1
Field: Format, FIXED, start_bit = 69, end_bit = 71
Field: ACL index, FIXED, start_bit = 54, end_bit = 68
Field: Flags, FIXED, start_bit = 43, end_bit = 53
Field: L4 proto, FIXED CNV, start_bit = 16, end_bit = 23
Field: Unknown, FLEX, start_bit = 0, end_bit = 15 Total bits = 53, format = 72 GMR used: 0
Col 3 LKBP Vector: 96C
Status: Running

-----
VMRs
----- VMR 0 -----
V: 7000C000 00000600 70
M: FFFFD800 0000FFFF F0
R: 80000104
Format: 00000003/00000007
ACL index: 00004003/00007FFF
L4 proto: 00000006/000000FF
Flags: 00000000/00000300
Packet Length: 00000070/0000FFFF
----- VMR 1 -----
V: 7000C000 00000600 68
M: FFFFD800 0000FFFF F8
R: 80000104
Format: 00000003/00000007
ACL index: 00004003/00007FFF
L4 proto: 00000006/000000FF
Flags: 00000000/00000300
Packet Length: 00000068/0000FFFF
----- VMR 2 -----
V: 7000C000 00000600 64
M: FFFFD800 0000FFFF FC

```

```

R: 80000104
Format: 00000003/00000007
ACL index: 00004003/00007FFF
L4 proto: 00000006/000000FF
Flags: 00000000/00000300
Packet Length: 00000064/0000FFFC
.
.
.
----- VMR 18 -----
V: 7000C000 00000000 00
M: FFFFC000 00000000 00
R: 80000110
Format: 00000003/00000007
ACL index: 00004003/00007FFF
L4 proto: 00000000/00000000
Flags: 00000000/00000000
Packet Length: 00000000/00000000

```

Related Commands

Command	Description
show pxf cpu policy-data	Displays QoS policy data index usage statistics.
show pxf cpu vcci	Displays VCCI to interface mapping information.

show pxf cpu police

To display all active policer policies in the Parallel eXpress Forwarding (PXF), including active interface and policing parameters, use the **show pxf cpu police** command in privileged EXEC mode.

show pxf cpu police [*policy-map-name*]

Syntax Description	<i>policy-map-name</i> (Optional) Policy for which you want to display PXF policing statistics.
---------------------------	---

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

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.

Usage Guidelines	If a policy name is not specified, the command displays policing statistics for all policy maps.
-------------------------	--

Examples	The following example shows the PXF policing statistics for a policy called policetest. The fields shown in the display are self-explanatory.
-----------------	---

```
Router# show pxf cpu police policetest
```

```
Policy policetest:
  Class: police_class
  Interface VCCI 0x9DD Output Policy:
    police 8000 8000 15000 conform-action transmit exceed-action drop violate-action drop

  Class: class-default
    *** No police action ***
```

Related Commands	Command	Description
	show pxf cpu vcci	Displays VCCI to interface mapping information.
	show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf cpu policy-data

To display Parallel eXpress Forwarding (PXF) policy data index usage statistics, use the **show pxf cpu policy-data** command in privileged EXEC mode.

show pxf cpu policy-data

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.

Examples The following example shows PXF policy data which is information related to the number of classes in a policy and the reservation of unique indexes to support match statistics and token buckets. Policy data index statistics are related to free match statistics indexes. Exhaustion of these indexes means no more policies can be created in the router. Secondary policy data indexes are related to free token bucket indexes. The fields shown in the display are self-explanatory.

```
Router# show pxf cpu policy-data

Service policy data index usage statistics:
Total groups = 9, pool_defragmented = TRUE.
  Group size      Chunk count
    1             0
    2             1
    4             1
    8             0
   16             1
   32             1
   64             1
  128             1
  256            1023
Total free count  = 262134.
Total chunk count = 262144.

Secondary policy data index usage statistics:
Total groups = 9, pool_defragmented = TRUE.
  Group size      Chunk count
    2             1
    4             1
    8             0
   16             1
   32             1
   64             1
  128             1
  256             1
  512            2047
Total free count  = 1048566.
Total chunk count = 1048576.
```

The Group size field is the number of policy classes. The Chunk count field is the number of blocks the group holds.

Related Commands	Command	Description
	show pxf cpu pbr action	Displays PBR actions configured in the PXF for all PBR route maps.
	show pxf cpu vcci	Displays VCCI to interface mapping information.

show pxf cpu qos

To display Parallel eXpress Forwarding (PXF) External Column Memory (XCM) contents related to a particular policy, use the **show pxf cpu qos** command in privileged EXEC mode.

show pxf cpu qos [**policy-map** *policy-name* | **vcci-maps**]

Cisco 10000 Series Router

show pxf cpu qos [*vcci* | **classifiers** | **flex-sum** | **policy-map** *policy-name* | **vcci-maps**]

Syntax Description

vcci	(Optional) Virtual Channel Circuit Identifier (VCCI). Information about this specified VCCI will be displayed.
classifiers	(Optional) Displays information about the criteria used to classify traffic.
flex-sum	(Optional) Displays summary information describing the amount of memory allocated in the PXF engine for use by the flexible key construction microcode. Note This option is only available on the Cisco 10000 series router for the PRE3.
policy-map <i>policy-name</i>	(Optional) Displays per-policy map information.
vcci-maps	(Optional) Displays VCCI map values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.3(7)XI1	This command was introduced on the Cisco 10000 series router for the PRE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Usage Guidelines

This command is useful in verifying the presence of a policy on interfaces and indexes programmed in the PXF.

Examples

The following example shows XCM contents related to a policy called police_test, which is defined as follows:

```
policy-map police_test
  class high-priority
  priority
  class low-priority
  set atm-clp
```

```
class class-default
  queue-limit 512
```

Router# **show pxf cpu qos police_test**

```
Output Polycmap: police_test
Vcci: A05  Flags: 4  Polycmap_index: 6  Polycmap_data_index: 12
OUT AT1/0/0.111 (0x71764660) ref_count 1
Output Action Table Contents for vcci 0xA05 - Polycmap index: 6
class-name: high-priority  class_index: 0  action_flags: 0x00
  srp_class_id: 0x01  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0
class-name: low-priority  class_index: 1  action_flags: 0x10
  srp_class_id: 0x00  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0
class-name: class-default  class_index: 2  action_flags: 0x00
  srp_class_id: 0x00  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0
```

Related Commands

Command	Description
show pxf cpu statistics qos	Displays match statistics for a service policy on an interface.

show pxf cpu queue

To display parallel express forwarding (PXF) queueing and link queue statistics, use the **show pxf cpu queue** command in privileged EXEC mode.

show pxf cpu queue [*interface* | *QID* | **summary**]

Cisco uBR10012 Universal Broadband Router

show pxf cpu queue [*interface* | *QID*]

Syntax Description

<i>interface</i>	(Optional) The interface for which you want to display PXF queueing statistics. This displays PXF queueing statistics for the main interface and all subinterfaces and permanent virtual circuits (PVCs). It also displays packets intentionally dropped due to queue lengths.
<i>QID</i>	(Optional) The queue identifier.
summary	(Optional) Displays queue scaling information such as: • Number of queues and recycled queues. • Number of available queue IDs (QIDs). • Number of packet buffers, recycled packet buffers, and free packet buffers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
12.3(23)BC1	The “Link Queues” output field for dynamic bandwidth sharing-enabled modular cable and wideband cable interfaces was added on the Cisco uBR10012 universal broadband router.
12.2(33)SB	This command was modified for virtual access interfaces (VAIs) and the output was modified for the summary option, and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SCB	The output of this command has been updated or re-arranged (compared to the VTMS version) for DOCSIS Weighted Fair Queuing (WFQ) Scheduler feature and implemented on the Cisco uBR10012 router.

Usage Guidelines

When neither the interface or QID is specified, the command displays queuing statistics for the route processors (RPs).

Cisco 10000 Series Router

The Cisco 10000 series router high-speed interfaces work efficiently to spread traffic flows equally over the queues. However, using single traffic streams in a laboratory environment might result in less-than-expected performance. To ensure accurate test results, test the throughput of the Gigabit Ethernet, OC-48 POS, or ATM uplink with multiple source or destination addresses. To determine if traffic is being properly distributed, use the **show pxf cpu queue** command.

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer allows you to specify a virtual access interface (VAI) as **viX.Y** in the **show pxf cpu queue** command. Instead, you must spell out the VAI as **virtual-access**.

For example, the router accepts the following command:

```
Router# show pxf cpu queue virtual-access2.1
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the VAI. For example, the router accepts the following command:

```
Router# show pxf cpu queue vi2.1
```

In Cisco IOS Release 12.2(33)SB and later releases, the output from the **show pxf cpu queue interface summary** command displays only the physical interface and the number of logical links. The output does not display the number of priority queues, class queues, and so on. This modification applies to the PRE3 and PRE4.

Cisco uBR10012 Universal Broadband Router

If dynamic bandwidth sharing (DBS) is enabled, the link queue information that is displayed refers to the specific type of interface that is configured—modular cable or wideband cable. The **summary** keyword option is not supported for the Cisco uBR10012 universal broadband router for wideband cable or modular cable interfaces. The **ATM** interface output is not available for this router.

See [Table 77](#) for descriptions of the **interface** keyword fields.

Table 77 *show pxf cpu queue Interface Option Field Descriptions*

Field	Description
<0-131071>	QID (queue identifier)
ATM	Asynchronous transfer mode interface Note The ATM interface output is not available for the Cisco uBR10012 universal broadband router.
BVI	Bridge-group virtual interface
Bundle	Cable virtual bundle interface
CTunnel	CTunnel interface
Cable	Cable modem termination service (CMTS) interface
DTI	Digital trunk interface
Dialer	Dialer interface
Ethernet	IEEE 802.3
FastEthernet	FastEthernet IEEE 802.3
GigabitEthernet	GigabitEthernet IEEE 802.3z
Group-Async	Async group interface
Loopback	Loopback interface
MFR	Multilink frame relay bundle interface

Table 77 *show pxf cpu queue Interface Option Field Descriptions (continued)*

Field	Description
Modular-Cable	Modular cable interface
Multilink	Multilink group interface
Null	Null interface
Port-channel	Ethernet channel of interfaces
RP	Forwarding path (FP) to route processing (RP) queues
Tunnel	Tunnel interface
Vif	Pragmatic general multicast (PGM) host interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual token ring
WB-SPA	line card to line card (LC-LC) queues
Wideband-Cable	Wideband CMTS interface

Examples

The following example shows PXF queueing statistics for an ATM interface when a QID is not specified. The sample output includes the dropped and dequeued packets for the VCs, and for classes associated with sessions that inherit queues from VCs.

```
Router# show pxf cpu queue atm 5/0/2
```

```
VCCI 2517: ATM non-aggregated VC 1/229, VCD 1, Handle 1, Rate 500 kbps
```

VCCI/ClassID	ClassName	QID	Length/Max	Res	Dequeues	Drops
0 2517/0	class-default	269	0/4096	11	3	0
0 2517/31	pak-priority	268	0/32	11	4	0

```
Queues Owned but Unused by VC (inheritable by sessions)
```

ClassID	ClassName	QID	Length/Max	Res	Dequeues	Drops
0	class-default	275	0/32	11	100	0
31	pak-priority	268	0/32	11	4	0

```
VCCI 2517: ATM non-aggregated VC 1/233, VCD 4, Handle 4, Rate 50 kbps
```

VCCI/ClassID	ClassName	QID	Length/Max	Res	Dequeues	Drops
0 2517/0	class-default	269	0/4096	11	3	0
0 2517/31	pak-priority	268	0/32	11	4	0

```
Queues Owned but Unused by VC (inheritable by sessions)
```

ClassID	ClassName	QID	Length/Max	Res	Dequeues	Drops
0	class-default	274	0/32	11	0	0
31	pak-priority	268	0/32	11	4	0

```
VCCI 2520: ATM non-aggregated VC 1/232, VCD 3, Handle 3, Rate 500 kbps
```

VCCI/ClassID	ClassName	QID	Length/Max	Res	Dequeues	Drops
0 2520/0	class-default	273	0/32	11	0	0
0 2520/31	pak-priority	268	0/32	11	4	0

VCCI 2519: ATM non-aggregated VC 1/231, VCD 2, Handle 2, Rate 500 kbps

VCCI/ClassID	ClassName	QID	Length/Max	Res	Dequeues	Drops
0 2519/0	class-default	272	0/32	11	0	0
0 2519/31	pak-priority	268	0/32	11	4	0

The following example displays PXF queuing statistics for QID 267:

Router# **show pxf cpu queue 267**

```

ID                                     : 267
Priority                               : Lo
CIR (in-use/configured)               : 0/65535
EIR (in-use/configured)               : 0/0
MIR (in-use/configured)               : 0/65535
Maximum Utilization configured        : no
Link                                   : 2
Flowbit (period/offset)               : 32768/32768
Burst Size                             : 1024 bytes
Bandwidth                              : 133920 Kbps
Channel                                : 0
Packet Descriptor Base                 : 0x00000100
ML Index                               : 0
Length/Average/Alloc                  : 0/0/32
Enqueues (packets/octet)              : 293352/9280610
Dequeues (packets/octet)              : 293352/9280610
Drops (tail/random/max_threshold)     : 0/0/0
Drops (no_pkt_handle/buffer_low)      : 0/0
WRED (weight/avg_smaller)              : 0/0
WRED (next qid/drop factor)            : 0/0
WRED (min_threshold/max_threshold/scale/slope):
precedence 0                          : 0/0/0/0
precedence 1                          : 0/0/0/0
precedence 2                          : 0/0/0/0
precedence 3                          : 0/0/0/0
precedence 4                          : 0/0/0/0
precedence 5                          : 0/0/0/0
precedence 6                          : 0/0/0/0
precedence 7                          : 0/0/0/0

```

Cisco uBR10012 Universal Broadband Router

The following examples show link queue information for specific wideband cable and modular cable interfaces when dynamic bandwidth sharing is enabled.

Modular Cable Interface

```

Router(config)# interface modular-cable 1/0/0:1
.
.
.

```

```

Router(config-if)# cable dynamic-bw-sharing
.
.
.

```

Router# **show pxf cpu queue modular-cable 1/0/0:1**

```

Link Queues :
QID   CIR(act/conf)   EIR       MIR       RF Chan.   Status
420   19661/19661     1/1       65535/65535  0          Inactive

```

Wideband Cable Interface

```
Router(config)# interface wideband-cable 1/0/0:0
.
.
.
Router(config-if)# cable dynamic-bw-sharing
.
.
Router# show pxf cpu queue wideband-cable 1/0/0:0
```

```
Link Queues :
QID   CIR(act/conf)      EIR           MIR           RF Chan.   Status
419   32768/32768         1/1           65535/65535   0          Inactive
566   19661/19661         1/1           65535/65535   1          Inactive
```

The following example shows service flow queue information for modular cable interfaces.

```
Router# show pxf cpu queue modular-cable 1/2/0:0
```

Cable Interface Queues:

QID	Len/Max	Dequeues	TailDrops	MinRt (Kbps)	Wt/Quantum	ShapeRt (Kbps)	FlowId
131147	0/255	190	0	0	1/240	0	58
131148	0/255	33820	0	0	1/10000	0	32824

Cable Service Flow Queues:

* Best Effort Queues

QID	Len/Max	Dequeues	TailDrops	MinRt (Kbps)	Wt/Quantum	ShapeRt (Kbps)	FlowId
131241	0/255	0	0	0	1/240	0	32881

* CIR Queues

QID	Len/Max	Dequeues	TailDrops	MinRt (Kbps)	Wt/Quantum	ShapeRt (Kbps)	FlowId
2049	254/255	131018	485751	99	1/1920	0	32880

* Low Latency Queues

QID	Len/Max	Dequeues	TailDrops
-----	---------	----------	-----------

Related Commands

Command	Description
cable dynamic-bw-sharing	Enables DBS on a specific modular cable or wideband cable interface.
show pxf cable controller	Displays information about the RF channel VTMS links and link queues.
show pxf cpu statistics queue	Displays PXF CPU queueing counters for all interfaces.

show pxf cpu reasm_index

To display information about reassembly of IP fragmented packets in the Parallel eXpress Forwarding (PXF), use the **show pxf cpu reasm_index** command in privileged EXEC mode.

show pxf cpu reasm_index [summary]

Syntax Description	summary	(Optional) Displays summary reassembly information of IP fragmented packets in the PXF.
--------------------	---------	---

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

Command History	Release	Modification
	12.2S	This command was introduced.

Examples The following example shows reassembly summary information. The fields shown in the display are self-explanatory.

```
Router# show pxf cpu reasm_index summary
```

```
Multilink Reassembly Index usage summary
```

```

Maximum  Used      Available
1251      0          1251
```

Related Commands	Command	Description
	ip virtual-reassembly	Enables VFR information on an interface.
	show ip virtual-reassembly	Displays VFR configuration and statistical information.

show pxf cpu statistics

To display Parallel eXpress Forwarding (PXF) CPU statistics, use the **show pxf cpu statistics** command in privileged EXEC mode.

```
show pxf cpu statistics [atom | backwalk | clear | diversion | drop [interface | vcci] | ip | ipv6 |
l2tp | mlp | qos [interface] | queue | rx [vcci] | security | arp-filter | drl [ cable-wan-ip |
wan-non-ip ]]
```

Cisco 10000 Series Router

```
show pxf cpu statistics diversion [ pxf [interface {interface | vcci}] | top number]
```

Syntax Description

atom	(Optional) Displays Any Transport over MPLS (AToM) statistics.
backwalk	(Optional) Displays backwalk requests statistics.
clear	(Optional) Clears PXF CPU statistics.
diversion	(Optional) Displays packets that the PXF diverted to the Route Processor (RP) for special handling.
drop [interface] [vcci]	(Optional) Displays packets dropped by the PXF for a particular interface or Virtual Circuit Connection Identifier (VCCI).
ip	(Optional) Displays IP statistics.
ipv6	(Optional) Displays IPv6 statistics.
l2tp	(Optional) Displays packet statistics for an L2TP Access Concentrator (LAC) (Optional) and L2TP Network Server (LNS).
mlp	(Optional) Displays multilink PPP (MLP) statistics.
pxf	(Optional) Displays packets that the PXF diverted to the Route Processor (RP). Available on the Cisco 10000 series router only.
pxf interface interface	(Optional) Displays per-interface PXF statistical information for the divert cause policer on a particular interface. Available on the Cisco 10000 series router only.
pxf interface vcci	(Optional) Displays per-VCCI PXF statistical information for the divert cause policer on a particular Virtual Circuit Connection Identifier (VCCI). Available on the Cisco 10000 series router only.
qos [interface]	(Optional) Displays match statistics for a service policy on an interface.
queue	(Optional) Displays queueing counters for all interfaces.
rx [vcci]	(Optional) Displays receive statistics for a VCCI.
security	(Optional) Displays ACL matching statistics.
top number	(Optional) Displays PXF statistical information for the number of top punters you specify. Available on the Cisco 10000 series router only. Valid values are from 1 to 100.
arp-filter	(Optional) Displays the ARP filter statistics.
drl	(Optional) Displays the divert rate limit.
cable-wan-ip	(Optional) Displays cable / wan-ip statistics for dropped packets.
wan-non-ip	(Optional) Displays DRL wan-non-ip statistics for dropped packets.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
12.2(28)SB	This command was introduced on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command was enhanced to display per-interface or per-VCCI PXF statistical information for the divert cause policer on a particular interface or VCCI, to display the top punters on an interface, and to display the provisioned burst size for any divert causes. These enhancements were implemented on the Cisco 10000 series router for the PRE2, PRE3, and PRE4.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers. Support for the Cisco uBR7225VXR router was added. The arp-filter , drl , cable-wan-ip , and wan-non-ip keywords were added .
12.2(33)SCE	This command was modified in Cisco IOS Release 12.2(33)SCE. The cable-wan-ip keyword was removed.

Usage Guidelines**Cisco 10000 Series Router Usage Guidelines**

- The **show pxf cpu statistics diversion** command displays statistical information about diverted packets. Divert causes with the string "ipv6..." display as "v6..." in the output of all **show pxf cpu statistics diversion** commands
- The output from the **show pxf cpu statistics diversion pxf** command was enhanced in Cisco IOS Release 12.2(33)SB to display the provisioned burst size for any divert causes.
- The **show pxf cpu statistics diversion pxf interface *interface*** command displays statistical information about the divert cause policer on a specific interface. The output of this command is similar to the output displayed at the aggregated level. This command enables you to see the traffic types being punted from an inbound interface, subinterface, and session.
- The **show pxf cpu statistics diversion pxf interface *vcci*** command displays statistical information about the divert cause policer on a specific VCCI. The output of this command is similar to the output displayed at the aggregated level. This command enables you to see the traffic types being punted from an inbound interface, subinterface, and session.
- The **show pxf cpu statistics diversion top *number*** command displays the interfaces, subinterfaces, and sessions with the highest number of punter packets.

Examples

The following example shows PXF queueing counters information. These are aggregate counters for all interfaces. The Total column is the total for all columns.

**Note**

If you are troubleshooting link utilization issues, the `deq_vtp_req`, `deq_flow_off`, and `deq_ocq_off` counters may indicate what is causing the versatile time management scheduler (VTMS) to slow down.

If you are troubleshooting overall PXF throughput issues, look at the High Next Time, Low Next Time, High Wheel Slot, and Low Wheel Slot counters.

Router# **show pxf cpu statistics queue**

Column 6 Enqueue/Dequeue Counters by Rows:

dbg Counters	0	1	2	3	4	5	6	7
Total								
=====	=====	=====	=====	=====	=====	=====	=====	=====
enq_pkt	0x0000FD9B	0x0000FC77	0x0000FE4A	0x0000FF81	0x0000FC53	0x0000FD2E	0x0000FF19	0x0000FDDE
0x0007EE55								
tail_drop_pkt	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
deq_pkt	0x0000FD47	0x0000FEF2	0x0000FCB3	0x0000FF65	0x0000FCE7	0x0000FC45	0x0000FEE7	0x0000FDF1
0x0007EE55								
deq_vtp_req	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
deq_flow_off	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
deq_ocq_off	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
enqdeq_conflict	0x0000003A	0x00000043	0x0000004A	0x00000039	0x0000003A	0x0000004F	0x00000036	0x00000031
0x000001F0								
bndl_pkt	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
frag_pkt	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
dbg_frag_drop	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
dbg_bndl_sem	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
context_inhibit	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
bfifo_enq_fail	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
dbg1	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
dbg2	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
dbg3	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
dbg4	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
dbg5	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
0x00000000								
dbg6	0x0000	0x0000	0x0000	0x0000	0x0000	0x0000	0x0000	0x0000
0x0000								
dbg7	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00

Column 7 Rescheduling State Counters by Rows:

dbg Counters	0	1	2	3	4	5	6	7
Total								


```

=====
=====
High Next Time 0x524E1100 0x524E1140 0x524E1140 0x524E1180 0x524E11C0 0x524E11C0 0x524E1200 0x524E1240 -
Low Next Time 0x524E1100 0x524E1140 0x524E1140 0x524E1180 0x524E11C0 0x524E1200 0x524E1200 0x524E1240 -
High Wheel Slot 0x00000844 0x00000845 0x00000846 0x00000846 0x00000847 0x00000848 0x00000848 0x00000849 -
Low Wheel Slot 0x00000844 0x00000845 0x00000846 0x00000846 0x00000847 0x00000848 0x00000848 0x00000849 -
DEQ_WHEEL 0x0001F5D0 0x0001F4BD 0x0001F56B 0x0001F6BF 0x0001F396 0x0001F3E8 0x0001F6BF 0x0001F4A7
0x000FA99B
DQ-lock Fails 0x0000039F 0x000003FD 0x000003B2 0x000003E1 0x000003CB 0x000003E2 0x000003FD 0x000003CD
0x00001EA6
TW_ENQ Fails 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
Q_SCHED 0x0000FACD 0x0000FC6B 0x0000FA38 0x0000FCE4 0x0000FA66 0x0000F994 0x0000FC62 0x0000FB8B
0x0007DA3B
FAST_SCHED 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
Q_DEACT 0x0000FB03 0x0000F852 0x0000FB33 0x0000F9DB 0x0000F930 0x0000FA54 0x0000FA5D 0x0000F91C
0x0007CF60
Q_ACTIVATE 0x0000F9B6 0x0000F8D4 0x0000FA6C 0x0000FBA9 0x0000F87E 0x0000F95B 0x0000FB0A 0x0000F9DE
0x0007CF60
Q_CHANGE 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG2 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG3 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG4 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
DEBUG5 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000

```

Table 78 describes the significant fields shown in the display.

Table 78 *show pxf cpu statistics queue Field Descriptions*

Field	Description
Column 6 Enqueue/Dequeue Counters by Rows:	
enq_pkt	Packets the PXF enqueued.
tail_drop_pkt	Packets the PXF tails dropped.
deq_pkt	Packets the PXF dequeued.
deq_vtp_req	Number of times a dequeue was inhibited due to the virtual traffic policer.
deq_flow_off	Numbers of times a dequeue was inhibited due to a flowoff from the line card.
deq_ocq_off	Number of times a dequeue was inhibited due to link level flow control.
enqdeq_conflict	Shows a dequeue failed due to an enqueue to the same queue in progress.
bndl_pkt	Count of packets that were fragmented.
frag_pkt	Count of fragments sent.
dbg_frag_drop	Count of invalid multilink PPP (MLP) fragment handles.
dbg_bndl_sem	Count of semaphore collision (used for MLP).

Table 78 *show pxf cpu statistics queue Field Descriptions (continued)*

Field	Description
context_inhibit	Number of times multilink transmit fragment processing was inhibited due to a lack of DMA resources.
bfifo_enq_fail	Count of bundle FIFO (BFIFO) enqueue failures.
Column 7 Rescheduling State Counters by Rows:	
High Next Time	Current next send time for the high priority wheel.
Low Next Time	Current next send time for the low priority wheel.
High Wheel Slot	Current high priority slot number.
Low Wheel Slot	Current low priority slot number.
DEQ_WHEEL	Count of successful dequeues from the timing wheel.
DQ-lock Fails	Count of timing wheel dequeue failures (both queue empty and race conditions).
TW ENG Fails	Timing wheel enqueue failures.
Q_SCHED	Count of queues scheduled/rescheduled onto the timing wheel.
FAST_SCHED	Count of queues fast scheduled/rescheduled onto the timing wheel.
Q_DEACT	Count of queue deactivations.
Q_ACTIVATE	Count of queue activations (activate state).
Q_CHANGE	Count of queue changes; for example, Route Processor (RP) inspired rates changes.

The following example displays PXF L2TP packet statistics.

**Note**

For L2TP Access Concentrator (LAC) operation, all statistics are applicable. For L2TP Network Server (LNS) operation, only the PPP Control Packets, PPP Data Packets, and PPP Station Packets statistics are meaningful.

```
Router# show pxf cpu statistics l2tp

LAC Switching Global Debug Statistics:
  PPP Packets           51648
  PPP Control Packets   51647
  PPP Data Packets      1
  Not IPv4 Packets      1
  IP Short Hdr Packets  1
  IP Valid Packets      0
  IP Invalid Packets    1
  DF Cleared Packets    0
  Path MTU Packets      0
  No Path MTU Packets   0
  Within PMTU Packets   0
  Fraggable Packets     0
  PMTU Pass Packets     0
  PMTU Fail Packets     0
  Encapped Packets      51648
```

L2TP Classification Global Debug Statistics:

```

LAC or Multihop Packets 151341
Multihop Packets        0
PPP Control Packets     51650
PPP Data Packets        99691
PPP Station Packets     151341

```

The following example displays match statistics for the police_test policy on an ATM interface. The Classmap Index differentiates classes within a policy while the Match Number differentiates match statements within a class.

Router# **show pxf cpu statistics qos atm 6/0/0.81801**

Classmap Index	Match Number	Pkts Matched	Bytes Matched

police_test (Output) service-policy :			
police_class (0)	0	0	0
	1	0	0
	2	0	0
	3	0	0
class-default (1)	0	0	0

Cisco 10000 Series Router

The following example displays the top 10 packet types diverted to the RP. The output displays the top punters by interface and by Layer 2 packet flow.

Router# **show pxf cpu statistics diversion top 10**

Top 10 punters by interface are:

Rate (pps)	Packets (diverted/dropped)	vcci	Interface
1	10/0	2606	Virtual-Access2.1

Last diverted packet type is none.

Top 10 punters by Layer 2 flow are:

Rate (pps)	Packets (diverted/dropped)	Interface	Layer 2 info
1	15/0	ATM2/0/3	vpi 128/vci 4096/vcci 2591

Last diverted packet type is oam_f4.

1	15/0	ATM2/0/3	vpi 128/vci 4096/vcci 2593
---	------	----------	----------------------------

Last diverted packet type is oam_f4.

Related Commands

Command	Description
platform c10k divert- policer	Configures the rate and burst size of the divert-policer.
show pxf statistics	Displays a summary of statistics in the PXF.

show pxf cpu subblocks

To display Parallel eXpress Forwarding (PXF) CPU statistics for a bridged subinterface (encapsulation type), use the **show pxf cpu subblocks** command in privileged EXEC mode.

show pxf cpu subblocks *interface-name*

Syntax Description	<i>interface-name</i>	Name of the interface.
---------------------------	-----------------------	------------------------

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

Command History	Release	Modification
	12.2(28)SB	This command was introduced on the Cisco 10000 series router.
	12.3(14)T	This command was enhanced to display more information for all subblocks.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples

The following example shows subblocks information for Gigabit Ethernet interface 7/0/0:

```
Router# show pxf cpu subblocks g7/0/0
```

```
GigabitEthernet7/0/0 is up
  ICB = 1C000, LinkId = 6, interface PXF, enabled
    link next_send:      0x37022604    channel number:      0
    link bandwidth mult:  33467         shift:              22
    link bandwidth mult:  33467         shift:              22
    link aggregate cir:   0x00000000    aggregate eir:       0x00000000
  IOS encapsulation type 1  ARPA
  Min mtu: 14      Max mtu: 1528
  VCCI mactable location = A3340000
  VCCI 9DB (802.1Q VLAN 1)
    icmp ipaddress 0.0.0.0      timestamp 0
    fib_root 0x0, fib_root_rpf 0x0 cicb_flags 0x00, flags/netmask 0x02
  VCCI 9DB (802.1Q VLAN 1)
    icmp ipaddress 0.0.0.0      timestamp 0
    fib_root 0x0, fib_root_rpf 0x0 cicb_flags 0x00, flags/netmask 0x02
```

The following example shows subblocks information for all interfaces:

```
Router# show pxf cpu subblocks PXF
```

Interface	Status	ICB	WQB_ID	Fwding	Enc	VCCI-map	VCCI	VC
Control Plane	up	0	1	PXF	0	A3000000	1	
ATM1/0/0	initiali	6000	3	disabl	33	A3040000	9CF	
ATM1/0/1	initiali	6001	4	disabl	33	A3060000	9D0	
ATM1/0/2	initiali	6002	5	disabl	33	A3080000	9D1	
ATM1/0/3	initiali	6003	6	disabl	33	A30A0000	9D2	
Serial2/0/0	initiali	A000	7	disabl	16	A3000004	9D3	
Serial2/0/1	initiali	A001	8	disabl	16	A3000008	9D4	
Serial2/0/2	initiali	A002	9	disabl	5	A300000C	9D5	
Serial2/0/3	initiali	A800	10	disabl	5	A3000010	9D6	
Serial2/0/4	initiali	A801	11	disabl	5	A3000014	9D7	
Serial2/0/5	initiali	A802	12	disabl	5	A3000018	9D8	

```

Serial2/0/6          initiali B000 13      disabl 5    A300001C 9D9
Serial2/0/7          initiali B001 14      disabl 5    A3000020 9DA
POS3/0/0             up      E000 15      PXF      5    A3000024 9DB
Serial4/0/0.1/1/1/1:0 up      12000 27     PXF      16   A3000040 9E7
Serial4/0/0.1/1/1/1:1 up      12001 28     PXF      16   A3000044 9E8
POS5/0/0             down    16000 16      disabl 5    A3000028 9DC
POS5/0/1             down    16001 17      disabl 5    A300002C 9DD
POS5/0/2             down    16002 18      disabl 5    A3000030 9DE
POS5/0/3             down    16003 19      disabl 5    A3000034 9DF
POS5/0/4             down    16004 20      disabl 5    A3000038 9E0
POS5/0/5             down    16005 21      disabl 5    A300003C 9E1
GigabitEthernet6/0/0 down    1A000 22      disabl 1    A32C0000 9E2 1
GigabitEthernet6/0/0.100 down    1A000 22      disabl 1    A32C0000 9EB 100
ATM8/0/0             up      22000 23      PXF      33   A33C0000 9E3
ATM8/0/0.1           up      22000 23      PXF      33   A33C0000 0 0/33
ATM8/0/0.2           up      22000 23      PXF      33   A33C0000 0 0/34
ATM8/0/0.100         up      22000 23      PXF      33   A33C0000 9EC 30/32
ATM8/0/0.200         up      22000 23      PXF      33   A33C0000 9ED 0/32
ATM8/0/1             down    22001 24      disabl 33   A33E0000 9E4
ATM8/0/2             down    22002 25      disabl 33   A3400000 9E5
ATM8/0/3             down    22003 26      disabl 33   A3420000 9E6
Multilink1           up      0      29      PXF      16   A3000048 2
Multilink2           down    0      36      disabl 16   A300005C 4
Multilink20          up      0      30      PXF      16   A300004C 3
Multilink60230       down    0      31      disabl 16   A3000050 9E9
Multilink60130       down    0      32      disabl 16   A3000054 9EA

```

Table 76 describes the fields shown in the display.

Table 79 *show pxf cpu subblocks Field Descriptions*

Field	Description
Interface	Identifies the interface or subinterface.
Status	Displays the status of the interface: - Administ—The interface has been shut down and is in the administrative down state. - Deleted—The subinterface has been removed from the router's configuration. - Down—The interface is down because of a cable or other connectivity problem. - Initiali—The interface is in the process of initializing. - Reset—The interface is currently being reset. - Up—The interface is up and passing traffic.
ICB	Displays the Interface Control Block (ICB) that is mapped to this interface.
WQB_ID	Displays the Work Queue Block (WQB) identifier for the interface.
Fwding	Displays whether traffic is being forwarded (PXF) or not (disable).

Table 79 *show pxf cpu subblocks Field Descriptions (continued)*

Field	Description
Enc	Identifies the type of encapsulation used on the interface. The most common encapsulation types are: 0 = None 1 = Ethernet ARPA 2 = Ethernet SAP 3 = 802.2 SNAP 5 = Serial, raw HDLC 8 = Serial, LAPB 9 = Serial, X.25 20 = Frame Relay 21 = SMDS 22 = MAC-level packets 27 = Logical Link Control (LLC) 2 28 = Serial, SDLC (primary) 30 = Async SLIP encapsulation 33 = ATM interface 35 = Frame Relay with IETF encapsulation 42 = Dialer encapsulation 46 = Loopback interface 51 = ISDN Q.921 59 = DOCSIS (previously known as MCNS) 61 = Transparent Mode 62 = TDM clear channel 64 = PPP over Frame Relay 65 = IEEE 802.1Q 67 = LAPB terminal adapter 68 = DOCSIS Cable Modem
VCCI-map	Displays the memory address for the Virtually Cool Common Index (VCCI) map table for this particular VCCI.
VCCI	Identifies the VCCI, in hexadecimal, assigned to the interface or subinterface.
VC	Identifies the virtual circuit (VC).

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
debug pxf	Displays PXF debugging output.
show ip mroute	Displays the contents of the IP multicast routing table.
show pxf cpu tbridge	Displays PXF CPU statistics for transparent bridging.
show pxf microcode	Displays identifying information for the microcode currently loaded on the PXF.

show pxf cpu vcci

To display Virtually Cool Common Index (VCCI) to interface mapping information on the Parallel eXpress Forwarding (PXF), use the **show pxf cpu vcci** command in privileged EXEC mode.

show pxf cpu vcci [summary]

Syntax Description	summary (Optional) Displays VCCI allocation information.
---------------------------	---

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

Command History	Release	Modification
	12.2S	This command was introduced.

Usage Guidelines	The VCCI is an index that uniquely identifies each interface or subinterface in the PXF and it maps that interface to the appropriate set of services and features. This command is useful to verify the number of VCCIs that are used and available.
	The Cisco 10000 series router has 65,536 VCCIs. A VCCI is assigned to each individual routed interface. A VCCI is not assigned to virtual template interfaces and loopbacks.

Examples	The following example shows how to display the number of used and available VCCIs. The fields shown in the display are self-explanatory.
	Router# show pxf cpu vcci summary

```
VCCI usage summary

          Maximum  Used    Available
Multilink VCCI    2500     0        2500
Other VCCI        63023    14       63009
```

Related Commands	Command	Description
	show pxf cpu policy-data	Displays QoS policy data index usage statistics.

show pxf crash

To display Parallel eXpress Forwarding (PXF) crash information, use the **show pxf crash** command in privileged EXEC mode.

show pxf crash

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.1(1)E	This command was introduced on the Cisco 10000 series router.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
	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.

Examples The following example shows crash information as a result of a PXF direct memory access (DMA) error. The PXF crash information is typically stored in bootflash.

```
Router# show pxf crash

Summary of bootflash:pxf_crashinfo_20060117-152035

Time of crash was 15:20:35 UTC Tue Jan 17 2006

PXF DMA Error - End of Descriptor Before Cmd Byte Length Exhausted

Current microcode:
  file=system:pxf/c10k2-11-ucode.108.0.0.0,
  version=108.0.0.0,
  description=Nightly Build Software created Sat 19-Nov-05 00:12
```

[Table 78](#) describes the significant fields shown in the display.

Table 80 *show pxf crash Field Descriptions*

Field	Description
Summary of bootflash:	Displays the filename in bootflash where the PXF crash information is stored. The filename format includes the date and time of the PXF crash.
Time of crash	Displays the date of the PXF crash.

Table 80 *show pxf crash Field Descriptions (continued)*

Field	Description
UTC	Displays the Universal Coordinated Time (UTC) of the PXF crash.
Current microcode	Displays identifying information for the microcode currently running on the PXF.

Related Commands

Command	Description
show pxf statistics	Displays a summary of PXF statistics.

show pxf dma

To display the current state of direct memory access (DMA) buffers, error counters, and registers on the Parallel eXpress Forwarding (PXF), use the **show pxf dma** command in privileged EXEC mode.

show pxf dma [**buffers** | **counters** | **reassemble** | **registers**]

Cisco 10000 Series Router (PRE3 only)

show pxf dma [**buffers** | **counters** | **reassemble** | **registers**] [**brief** | **config** | **errors** | **status**]

Syntax Description	
buffers	(Optional) Displays PXF DMA buffers information.
counters	(Optional) Displays packet and error counters for the PXF DMA engine.
reassemble	(Optional) Displays PXF reassembly table usage information.
registers	(Optional) Displays PXF DMA registers information.
brief	(Optional) Displays PXF DMA information, including the initialization state of each block in the PXF API and any errors that occurred. Note This option is available on the PRE3 only.
config	(Optional) Displays a configuration summary of the registers in each of the PXF DMA blocks. Note This option is available on the PRE3 only.
errors	(Optional) Displays the errors that occurred in each of the PXF DMA blocks. Note This option is available on the PRE3 only.
status	(Optional) Displays the initialization state of each PXF DMA block. In normal operation, all blocks display the enabled state. Note This option is available on the PRE3 only.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series router for the PRE2.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router for the PRE3.

Examples

The following example shows PXF DMA buffers information:

Router# **show pxf dma buffers**

PXF To-RP DMA Ring Descriptors & Buffers:

	Descriptor Address	Buffer Address	Buffer Length(b)	Descriptor Flags
0	0x0CA06340	0x0AC097C0	512	0x0002
1	0x0CA06350	0x0AC088C0	512	0x0002
2	0x0CA06360	0x0AC07C40	512	0x0002
3	0x0CA06370	0x0AC0B5C0	512	0x0002
4	0x0CA06380	0x0AC0CC40	512	0x0002
5	0x0CA06390	0x0AC08640	512	0x0002
6	0x0CA063A0	0x0AC0C240	512	0x0002
7	0x0CA063B0	0x0AC08B40	512	0x0002
8	0x0CA063C0	0x0AC0AE40	512	0x0002
9	0x0CA063D0	0x0AC0BAC0	512	0x0002
10	0x0CA063E0	0x0AC0C9C0	512	0x0002
11	0x0CA063F0	0x0AC09CC0	512	0x0002
12	0x0CA06400	0x0AC0C740	512	0x0002
13	0x0CA06410	0x0AC0A6C0	512	0x0002
14	0x0CA06420	0x0AC0B0C0	512	0x0002
15	0x0CA06430	0x0AC09040	512	0x0002
16	0x0CA06440	0x0AC0A440	512	0x0002
17	0x0CA06450	0x0AC065C0	512	0x0002
18	0x0CA06460	0x0AC06FC0	512	0x0002
19	0x0CA06470	0x0AC06340	512	0x0002
20	0x0CA06480	0x0AC07240	512	0x0002
21	0x0CA06490	0x0AC092C0	512	0x0002
22	0x0CA064A0	0x0AC0D140	512	0x0002
23	0x0CA064B0	0x0AC0C4C0	512	0x0002
24	0x0CA064C0	0x0AC07740	512	0x0002
25	0x0CA064D0	0x0AC09540	512	0x0002
26	0x0CA064E0	0x0AC0A940	512	0x0002
27	0x0CA064F0	0x0AC06840	512	0x0002
28	0x0CA06500	0x0AC08140	512	0x0002
29	0x0CA06510	0x0AC06D40	512	0x0002
30	0x0CA06520	0x0AC07EC0	512	0x0002
31	0x0CA06530	0x0AC0ABC0	512	0x0003

PXF From-RP DMA Ring Descriptors & Buffers:

	Descriptor Address	Buffer Address	Buffer Length(b)	Descriptor Flags	Context Bit
0	0x0CA06580	0x00000000	0	0x0000	Not set
1	0x0CA06590	0x00000000	0	0x0000	Not set
2	0x0CA065A0	0x00000000	0	0x0000	Not set
3	0x0CA065B0	0x00000000	0	0x0000	Not set
4	0x0CA065C0	0x00000000	0	0x0000	Not set
5	0x0CA065D0	0x00000000	0	0x0000	Not set
6	0x0CA065E0	0x00000000	0	0x0000	Not set
7	0x0CA065F0	0x00000000	0	0x0000	Not set
8	0x0CA06600	0x00000000	0	0x0000	Not set
9	0x0CA06610	0x00000000	0	0x0000	Not set
10	0x0CA06620	0x00000000	0	0x0000	Not set
11	0x0CA06630	0x00000000	0	0x0000	Not set
12	0x0CA06640	0x00000000	0	0x0000	Not set
13	0x0CA06650	0x00000000	0	0x0000	Not set
14	0x0CA06660	0x00000000	0	0x0000	Not set
15	0x0CA06670	0x00000000	0	0x0001	Not set

Table 76 describes the fields shown in the display.

Table 81 *show pxf dma Field Descriptions*

Field	Description
Descriptor Address	Memory address pointing to the descriptor for this buffer.
Buffer Address	Address of this buffer in memory.
Buffer Length	Length, in bytes, of this particular buffer.
Descriptor Flags	Internal flags identifying this buffer's use and status.
Context Bit	State of the context bit which is set when the buffer is currently in use by a context (the basic unit of packet processing).

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf cpu	Displays PXF CPU statistics.
show pxf microcode	Displays the microcode version running on the PXF.

show pxf feature cef

To display Parallel eXpress Forwarding (PXF) routing feature tables for Cisco Express Forwarding, use the **show pxf feature cef** command in user EXEC or privileged EXEC mode.

show pxf feature cef *entry*

Syntax Description

<i>entry</i>	Display the PXF entry.
--------------	------------------------

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)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.

Examples

The following is sample output from the **show pxf feature cef** command. The fields shown in the display are self-explanatory.

Router# **show pxf feature cef entry**

```
Shadow 16-4-4-8 PXF Mtrie:
  41 leaves, 1968 leaf bytes, 15 nodes, 267000 node bytes
  5 invalidations
  46 prefix updates
  refcounts: 66746 leaf, 66720 node
```

Prefix/Length	Refcount	Parent
0.0.0.0/0	62282	
0.0.0.0/32	3	0.0.0.0/0
171.22.12.128/27	34	0.0.0.0/0
171.22.12.128/32	3	171.22.12.128/27
171.22.12.129/32	3	171.22.12.128/27
171.22.12.130/32	3	171.22.12.128/27
171.22.12.131/32	3	171.22.12.128/27
171.22.12.147/32	3	171.22.12.128/27

Related Commands

Command	Description
show pxf feature nat	Displays PXF routing feature tables for NAT.

show pxf feature cef vrf

To display the routing feature tables for Virtual Private Network (VPN) routing and forwarding instances (VRFs) on the Parallel eXpress Forwarding (PXF) path, use the **show pxf feature cef vrf** command in privileged EXEC mode.

show pxf feature cef vrf *vpn-name*

Syntax Description	<i>vpn-name</i>	Name of the VPN to display.
--------------------	-----------------	-----------------------------

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

Command History	Release	Modification
	12.2(15)B	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines	Use this command to display VRF PXF routing feature tables for a specified VPN for Cisco Express Forwarding. This command also displays information about prefix and MTRIE resource usage.
------------------	--

Examples	The following is sample output for the show pxf feature cef vrf command when it is used to display information about VRF vpn1:
----------	---

Router# **show pxf feature cef vrf vpn1**

```
Shadow 8-8-4-4-8 PXF Mtrie:
  51 leaves, 2448 leaf bytes, 92 nodes, 56352 node bytes
  10 invalidations
  61 prefix updates
  refcounts: 3666 leaf, 3733 node
```

Prefix/Length	Refcount	Parent	Address	Shadow
0.0.0.0/32	3		0xC0047218	0x62CAF2E8
10.5.0.0/16	558		0xC0047278	0x62CAF108
10.5.0.0/32	3	10.5.0.0/16	0xC0047268	0x62CAEE08
10.5.0.1/32	3	10.5.0.0/16	0xC0047260	0x62CAEA18
10.5.0.2/32	3	10.5.0.0/16	0xC0047388	0x62CAEA48
10.5.0.255/32	3	10.5.0.0/16	0xC0047270	0x62CAF0D8
10.30.1.0/16	288		0xC0047360	0x62CAEB38
10.30.1.1/32	3	10.30.1.0/16	0xC0047350	0x62CAEB98
10.70.0.0/32	3		0xC00472C0	0x62CAEEF8
10.70.1.1/32	3		0xC0047358	0x62CAEB68
10.70.1.2/32	3		0xC0047368	0x62CAEB08
10.70.1.3/32	3		0xC0047370	0x62CAEAD8
10.70.1.4/32	3		0xC0047378	0x62CAEA88
70.1.1.5/32	3		0xC0047380	0x62CAEA78
224.0.0.0/24	3		0xC0047228	0x62CAF288
255.255.255.255/32	3		0xC0047220	0x62CAF2B8

=====

5 routes with less specific overlapping parent route

Table 82 describes the significant fields shown in the display.

Table 82 *show pxf feature cef vrf Field Descriptions*

Field	Description
Shadow 8-8-4-4-8 PXF Mtrie	MTRIE lookup table index structures.
51 leaves	All created leaves for all MTRIEs.
2448 leaf bytes	Leaf byte counter. When a new leaf is created, the leaf byte counter is incremented by the size of the leaf structure.
92 nodes	All created nodes for all MTRIEs.
56352 node bytes	Node byte counter. When a new node is created, the node byte counter is incremented.
10 invalidations	Invalidations counter. When a route (represented by a leaf) is deleted from an MTRIE, the invalidations counter is incremented. This counter includes all MTRIEs.
61 prefix updates	IP prefix counter. When an IP prefix (represented by a leaf) is added to the MTRIE, the IP prefix counter is incremented. This counter includes all MTRIEs.
refcounts	Counters associated with references between leaves.
3666 leaf	MTRIEs have a leaf lock and a leaf free function. The leaf lock function increments the leaf refcount. The leaf free function decrements the leaf refcount. The leaf lock and leaf free functions prevent a leaf from being freed (deleted) while the leaf is still being referenced. This counter includes all MTRIEs.
3733 node	Node counter. When a child node is added to another node, the node to which the child node is added becomes a parent node. The node counter is decremented when a child node is deleted. This counter includes all MTRIEs.
Prefix/Length	The IP address and subnet mask of a leaf.
Refcount	The number of leaves that reference a specified leaf. The refcount counter is incremented when the leaf lock function is called and decremented when the leaf free function is called.
Parent	When you add a less specific route to a more specific route, the more specific route has a back pointer that points to the less specific route.
Address	The address of the memory for the specified leaf.
Shadow	The shadow address in Route Processor memory for the specified leaf.

Related Commands

Command	Description
show pxf feature cef	Displays PXF routing feature tables for CEF.
show pxf feature nat	Displays PXF routing feature tables for NAT.

show pxf feature nat

To display Parallel eXpress Forwarding (PXF) routing tables for Network Address Translation (NAT), use the **show pxf feature nat** command in user EXEC or privileged EXEC mode.

show pxf feature nat [**entry** | **stat** | **tcp**]

Syntax Description	entry	Displays NAT information.
	stat	Displays NAT processing information.
	tcp	Displays NAT TCP logging information.

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

Command History	Release	Modification
	12.1(1)E	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)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.

Examples The following is sample output from the **show pxf feature nat** command. The fields shown in the display are self-explanatory.

Router# **show pxf feature nat**

```

--- 171.22.12.175      192.168.0.129      ---      ---
--- 171.22.12.163      192.168.0.7        ---      ---
--- 171.22.12.161      192.168.0.13       ---      ---
--- 171.22.12.162      192.168.0.3        ---      ---
--- 171.22.12.165      192.168.0.8        ---      ---
--- 171.22.12.168      192.168.0.14       ---      ---
--- 171.22.12.170      192.168.0.12       ---      ---
--- 171.22.12.166      192.168.0.15       ---      ---
--- 171.22.12.164      192.168.0.16       ---      ---

```

Related Commands	Command	Description
	show pxf feature cef	Displays PXF routing feature tables for Cisco Express Forwarding.

show pxf interface

To display a summary of the interfaces on the router and the Parallel eXpress Forwarding (PXF) features and capabilities enabled on these interfaces, use the **show pxf interface** command in privileged EXEC mode.

```
show pxf interface interface-name [detail]
```

Syntax Description	interface-name	Name of the interface.
	detail	(Optional) Displays detailed information for all PXF interfaces on the router.

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

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
	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	If you do not specify an interface, the command displays a summary of the statistics for all PXF interfaces on the router.
------------------	--

Examples The following example shows PXF statistics for serial interface 1/0/0. The significant fields shown in the display are self-explanatory.

```
Router# show pxf interface s1/0/0

ed10#sho pxf interface s1/0/0
Serial1/0/0 is up, enabled, PXF enabled, IOS encap PPP      (16)
  Last clearing of Serial1/0/0 counters: 00:06:29
    91 packets input, (1934 bytes)

Total PXF input errors (pkts/bytes):          0/0

PXF output queues:
      Class      ID    Length/Max    Outputs (pkts/bytes)    Drops
    0 class-default  276    0/1024         0/0                    0
    15              -   275    0/32         91/1953                 0

Slot 1/0: FBB Rx:0x00000000 OCQ debug:0x00001040, qN_entry_cnt[5:0]: 0
          PXF DMA RE drops: 0/0, Null config drops: 0/0
          Last clearing of slot 1/0 counters: 00:06:29
```

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf microcode

To display identifying information for the microcode currently loaded on the Parallel eXpress Forwarding (PXF), use the **show pxf microcode** command in privileged EXEC mode.

show pxf microcode

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI.

Examples The following example shows the microcode version that is currently loaded on the PXF:

```
Router# show pxf microcode

PXF complex: 4 Toasters 8 Columns total
PXF processor tmc0 is running.
PXF processor tmc1 is running.
PXF processor tmc2 is running.
PXF processor tmc3 is running.

Loaded microcode: system:pxf/c10k2-11-ucode.6.1.3
    Version: 6.1.3
    Release Software created Sun 20-Nov-05 14:06
    Signature: 0d2b395c1083872793586f9cec47d7b3
    Microcode load attempted 1 time(s), latest 2w6d ago
    tmc0 FG_PC=0 BG_PC=6 WDog=1024 MinPhase=23 SecPreScalerTimer=11542680 MS
ecPreScalerTimer=153600
    tmc1 FG_PC=0 BG_PC=6 WDog=1024 MinPhase=23 SecPreScalerTimer=11542680 MS
ecPreScalerTimer=153600
    tmc2 FG_PC=0 BG_PC=6 WDog=1024 MinPhase=23 SecPreScalerTimer=11542680 MS
ecPreScalerTimer=153600
    tmc3 FG_PC=0 BG_PC=6 WDog=1024 MinPhase=23 SecPreScalerTimer=11542680 MS
ecPreScalerTimer=154
```

[Table 83](#) describes the fields shown in the display.

Table 83 *show pxf microcode Field Descriptions*

Field	Description
PXF complex	The number of PXF processors, their associate memory columns, and their current status.
Loaded microcode	The source and filename for the microcode that is currently loaded on the PXF processor.
Version	The microcode version.

Table 83 *show pxf microcode Field Descriptions (continued)*

Field	Description
Release Software created	The time and date the current microcode was compiled.
Signature	The signature in the microcode version.
Microcode load attempted	The number of times the PXF processor has loaded the microcode since the Cisco IOS image was loaded at system boot. Also, shows the time (in days and hours) since the last successful load of the microcode.
tmc#	The current program counters and configuration for the PXF processors.

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf cpu statistics	Displays PXF CPU statistics.
show pxf dma	Displays PXF DMA information.

show pxf netflow

To display the NetFlow Parallel eXpress Forwarding (PXF) counters, use the **show pxf netflow** command in privileged EXEC mode.

show pxf netflow

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI.

Examples The following example shows the NetFlow PXF statistics. The fields shown in the display are self-explanatory.

```
Router# show pxf netflow

NetFlow debug counters
  timeout activity:      0
  timeout inactivity: 9785
  forced age:           0
  export busy:          1
  export locked:        62
  export noswap:         2
  accumulate:           1296898
  new flow:              9808

(unreliable) ICM counters
  records pending :     0
  live flows :         0

NetFlow PXF Config Registers
  PXF Inactive Timeout: 90000
  PXF Active Timeout:   90000
```

Related Commands	Command	Description
	show pxf cpu statistics	Displays PXF CPU statistics.
	show pxf statistics	Displays chassis-wide, summary PXF statistics.

show pxf stall-monitoring

To display the configuration and operating status details of the PXF stall monitor (PSM), use the **show pxf stall-monitoring** command in privileged EXEC mode. The **show pxf stall-monitoring** command also displays the number of stalls on the PSM after it was last enabled.

```
show pxf stall-monitoring [counters | reset { active-status | cob-fib | cob-tib | pxf-drop } subslot
sub-slot]
```

Syntax Description	counters	Displays statistical information for all counters.
	reset	Displays the following counters: active-status—Displays the active status on the specified subslot. cob-fib—Displays the Cobalt FIB counter on the specified subslot. cob-tib—Displays the Cobalt TIB counter on the specified subslot. pxf-drop—Displays the PXF per RSRC drop counter on the specified subslot. subslot sub slot—Displays information about the specified subslot.

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

Command History	Release	Modification
	12.2(33)XNE	This command was introduced.

Examples The following example displays a sample output of the **show pxf stall-monitoring** command:

```
Router# show pxf stall-monitoring

pxf stall-monitoring : Enabled
Stall History
=====
Stall Threshold Configuration
=====
Primary Action = LC-reset Threshold = 3 (default)
Primary Action = HT-reset Threshold = 3 (default)

Secondary action = SSO SwitchOverRouter#
```

The fields displayed are self-explanatory.

The following example displays a sample output of the **show pxf stall-monitoring counters** command:

```
Router# show pxf stall-monitoring counters

To RP Counters
=====
IOS To RP Counter = 20665
PXF To RP Drop Counter = 0
Current Counter Values
```

```

=====
Slot 0 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 0 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 1 Subslot 0 Cob TIB = 2368 Cob FIB = 0 PXF Drop = 0
Slot 1 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 2 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 2 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 3 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 3 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 4 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 4 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 5 Subslot 0 Cob TIB = 6162 Cob FIB = 6204 PXF Drop = 0
Slot 5 Subslot 1 Cob TIB = 6101 Cob FIB = 6065 PXF Drop = 0
Slot 5 Subslot 2 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 5 Subslot 3 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 7 Subslot 0 Cob TIB = 8402 Cob FIB = 8402 PXF Drop = 0
Slot 7 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 8 Subslot 0 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Slot 8 Subslot 1 Cob TIB = 0 Cob FIB = 0 PXF Drop = 0
Line Card Participant Status
=====
Slot 1 Subslot 0 = 1
Slot 1 Subslot 1 = 0
Slot 2 Subslot 0 = 0
Slot 2 Subslot 1 = 0
Slot 3 Subslot 0 = 0
Slot 3 Subslot 1 = 0
Slot 4 Subslot 0 = 0
Slot 4 Subslot 1 = 0
Slot 5 Subslot 0 = 0
Slot 5 Subslot 1 = 1
Slot 5 Subslot 2 = 0
Slot 5 Subslot 3 = 0
Slot 7 Subslot 0 = 1
Slot 7 Subslot 1 = 0
Slot 8 Subslot 0 = 1
Slot 8 Subslot 1 = 0
Line Card Active Status
=====
Slot 1 Subslot 0 = 0
Slot 1 Subslot 1 = 0
Slot 2 Subslot 0 = 0
Slot 2 Subslot 1 = 0
Slot 3 Subslot 0 = 0
Slot 3 Subslot 1 = 0
Slot 4 Subslot 0 = 0
Slot 4 Subslot 1 = 0
Slot 5 Subslot 0 = 0
Slot 5 Subslot 1 = 1
Slot 5 Subslot 2 = 0
Slot 5 Subslot 3 = 0
Slot 7 Subslot 0 = 0
Slot 7 Subslot 1 = 0
Slot 8 Subslot 0 = 0
Slot 8 Subslot 1 = 0

```

The fields displayed are self-explanatory.

The following example displays a sample output of the **show pxf stall-monitoring reset** command:

```

Router# show pxf stall-monitoring reset active-status subslot 1/0

pxf stall-monitoring : Enabled
0

```

Related Commands

Command	Description
hw-module pxf stall-monitoring	Enables PXF stall monitor on the Cisco 10000 series router and configures default threshold values before the LC and HTDP resets.

show pxf statistics

To display summary Parallel eXpress Forwarding (PXF) statistics, use the **show pxf statistics** command in privileged EXEC mode.

show pxf statistics { context | diversion | drop [detail] | ip | ipv6 }

Syntax Description	context	Displays context statistics.
	diversion	Displays traffic diverted from the PXF.
	drop [detail]	Displays packets dropped by the PXF. The detail option provides detailed information.
	ip	Displays IP and ICMP statistics.
	ipv6	Displays IPv6 statistics.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.0(22)S	This command was introduced on the Cisco 10000 series router.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples

The following example shows a summary of PXF IP statistics:

```
Router# show pxf statistics ip

Chassis-wide PXF forwarding counts
  IP inputs 0, forwarded 0, punted 0
  IP dropped 0, no adjacency 0, no route 0
  IP unicast RPF 0, unresolved 0

  ICMP created 0, Unreachable sent 0, TTL expired sent 0
  ICMP echo requests 0, replies sent 0
  ICMP checksum errors 0

  IP packets fragmented 0, total fragments 0, failed 0
  IP don't-fragment 0, multicast don't-fragment 0

  IP mcast total 0, switched 0, punted 0, failed 0
  IP mcast drops 0, RPF 0, input ACL 0, output ACL + taildrops 0
Last clearing of PXF forwarding counters:never
```

The following example shows a summary of PXF statistics for dropped packets:

```
Router# show pxf statistics drop

PXF input drops:
  Unassigned drops (pkts/bytes):                0/0
Last clearing of drop counters: never
```

The following example shows detailed PXF statistics for dropped packets:

Router# **show pxf statistics drop detail**

PXF input drops:

Unassigned drops (pkts/bytes): 0/0

PXF Unassigned input drop details:

(These input drops are not assigned to a particular PXF interface.)

	packets	bytes
generic	0	0
mpls_no_eos	0	0
fib_zero_dest	0	0
fib_drop_null	0	0
fib_icmp_no_adj	0	0
fib_icmp_bcast_dst	0	0
mfib_ttl_0	0	0
mfib_disabled	0	0
mfib_rpf_failed	0	0
mfib_null_oif	0	0
tfib_rp_flag	0	0
tfib_eos_violation	0	0
tfib_nonip_expose	0	0
tfib_label_invalid	0	0
tfib_path_unknown	0	0
tfib_nonip_ttl_exp	0	0
icmp_unrch_interval	0	0
icmp_on_icmp	0	0
icmp_bad_hdr	0	0
icmp_multicast	0	0
icmp_frag	0	0
macr_bad_tag_num	0	0
no_touch	0	0
eng_id_0	0	0
no_pkt_handles	0	0
l2_unsupp_drop	0	0
ipm_replay_full	0	0
bad_atm_arp	0	0
nested_fragmentation	0	0
l2less drop packets	0	0
l2tp_payload_encap	0	0
re_bit[00]	0	0
[01]	0	0
[02]	0	0
[03]	0	0
[04]	0	0
[05]	0	0
[06]	0	0
[07]	0	0
[08]	0	0
[09]	0	0
[10]	0	0

.
.
.

The following example shows summarized statistics for traffic diverted from the PXF:

```
Router# show pxf statistics diversion
```

```
Diversion Cause Stats:
```

```
divert      = 0
encap       = 0
clns_isis   = 0
clns        = 0
cdp         = 0
cgmpp       = 0
arp         = 1
rarp        = 0
mpls_ctl    = 0
keepalive   = 0
ppp_cntrl   = 449
fr_lmi      = 0
atm ilmi    = 0
oam f4      = 0
oam f5 ete  = 0
oam f5 seg  = 0
mlfr lip    = 0
```

```
.
.
.
```

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf cpu statistics	Displays PXF CPU statistics.

show pxf xcm

To display Parallel eXpress Forwarding (PXF) External Column Memory (XCM) information, use the **show pxf xcm** command in privileged EXEC mode.

show pxf xcm

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.
	12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI.

Examples The following example shows XCM information for each PXF processor:

```
Router# show pxf xcm

Toaster 0:
  Number of Columns: 2
  Proc ID: 0x00000004 = TMC_X72
  ASIC Revision: 0x00000001 = T3-ECC
  XCM0 type:FCRAM, size = 67108864
  ECC is enabled for column 0
    XCM AB Config Register: 0x024703B9
    XCM CD Config Register: 0x024703B9
    XCM Exception Type Register: 0x00000000
    FCRAM-A Counters
      Number of ECC single bit errors: 0
    FCRAM-B Counters
      Number of ECC single bit errors: 0
    FCRAM-C Counters
      Number of ECC single bit errors: 0
    FCRAM-D Counters
      Number of ECC single bit errors: 0
  XCM1 type:FCRAM, size = 67108864
  ECC is enabled for column 1
    XCM AB Config Register: 0x024703B9
    XCM CD Config Register: 0x024703B9
    XCM Exception Type Register: 0x00000000
    FCRAM-A Counters
      Number of ECC single bit errors: 0
    FCRAM-B Counters
      Number of ECC single bit errors: 0
    FCRAM-C Counters
      Number of ECC single bit errors: 0
    FCRAM-D Counters
      Number of ECC single bit errors: 0
Toaster 1:
  Number of Columns: 2
  Proc ID: 0x00000004 = TMC_X72
  ASIC Revision: 0x00000001 = T3-ECC
```

```

XCM0 type:FCRAM, size = 67108864
ECC is enabled for column 0
  XCM AB Config Register: 0x024703B9
  XCM CD Config Register: 0x024703B9
  XCM Exception Type Register: 0x00000000
  FCRAM-A Counters
    Number of ECC single bit errors: 0
  FCRAM-B Counters
    Number of ECC single bit errors: 0
  FCRAM-C Counters
    Number of ECC single bit errors: 0
  FCRAM-D Counters
    Number of ECC single bit errors: 0
XCM1 type:FCRAM, size = 67108864
ECC is enabled for column 1
  XCM AB Config Register: 0x024703B9
  XCM CD Config Register: 0x024703B9
  XCM Exception Type Register: 0x00000000
  FCRAM-A Counters
    Number of ECC single bit errors: 0

  FCRAM-B Counters
    Number of ECC single bit errors: 0
  FCRAM-C Counters
    Number of ECC single bit errors: 0
  FCRAM-D Counters
    Number of ECC single bit errors: 0
Toaster 2:
  Number of Columns: 2
  Proc ID: 0x00000004 = TMC_X72
  ASIC Revision: 0x00000001 = T3-ECC
  XCM0 type:FCRAM, size = 67108864
  ECC is enabled for column 0
    XCM AB Config Register: 0x024703B9
    XCM CD Config Register: 0x024703B9
    XCM Exception Type Register: 0x00000000
    FCRAM-A Counters
      Number of ECC single bit errors: 0
    FCRAM-B Counters
      Number of ECC single bit errors: 0
    FCRAM-C Counters
      Number of ECC single bit errors: 0
    FCRAM-D Counters
      Number of ECC single bit errors: 0
  XCM1 type:FCRAM, size = 67108864
  ECC is enabled for column 1
    XCM AB Config Register: 0x024703B9
    XCM CD Config Register: 0x024703B9
    XCM Exception Type Register: 0x00000000
    FCRAM-A Counters
      Number of ECC single bit errors: 0
    FCRAM-B Counters
      Number of ECC single bit errors: 0
    FCRAM-C Counters
      Number of ECC single bit errors: 0
    FCRAM-D Counters
      Number of ECC single bit errors: 0
Toaster 3:
  Number of Columns: 2
  Proc ID: 0x00000004 = TMC_X72
  ASIC Revision: 0x00000001 = T3-ECC
  XCM0 type:FCRAM, size = 67108864
  ECC is enabled for column 0
    XCM AB Config Register: 0x024703B9

```

```

XCM CD Config Register: 0x024703B9
XCM Exception Type Register: 0x00000000
FCRAM-A Counters
Number of ECC single bit errors: 0
FCRAM-B Counters
Number of ECC single bit errors: 0
FCRAM-C Counters
Number of ECC single bit errors: 0
FCRAM-D Counters
Number of ECC single bit errors: 0
XCM1 type:FCRAM, size = 67108864
ECC is enabled for column 1
XCM AB Config Register: 0x024703B9
XCM CD Config Register: 0x024703B9
XCM Exception Type Register: 0x00000000
FCRAM-A Counters
Number of ECC single bit errors: 0
FCRAM-B Counters
Number of ECC single bit errors: 0
FCRAM-C Counters
Number of ECC single bit errors: 0
FCRAM-D Counters
Number of ECC single bit errors: 0

```

Table 84 describes the fields shown in the display.

Table 84 *show pxf xcm Field Descriptions*

Field	Description
The following fields appear for each PXF processor.	
Toaster #	Identifies the PXF processor.
Number of Columns	Displays the number of memory columns on the PXF processor.
Proc ID	Displays the processor type (TMC is Toaster Memory Column).
ASIC Revision	Displays the internal version number of the PXF processor.
The following fields appear for each XCM memory column.	
XCM type	Displays the type and size, in bytes, of memory used in this particular column.
ECC is enabled for column	Displays whether Error Code Correction (ECC) checking is enabled or disabled for this memory column.
XCM Config Register and XCM Exception Type Register	Displays the contents of these two registers for the memory column.
Number of ECC single bit errors	Displays the number of single-bit errors detected in memory.

Related Commands

Command	Description
show pxf cpu	Displays PXF CPU statistics.
show pxf microcode	Displays the microcode version currently loaded on the PXF.

show route-map ipc

To display counts of the one-way route map interprocess communication (IPC) messages sent from the rendezvous point (RP) to the Versatile Interface Processor (VIP) when NetFlow policy routing is configured, use the **show route-map ipc** command in privileged EXEC mode.

show route-map ipc

Syntax Description	This command has no arguments or keywords.
---------------------------	--

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

Command History	Release	Modification
	12.0(3)T	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	This command displays the counts of one-way route map IPC messages from the RP to the VIP when NetFlow policy routing is configured. If you execute this command on the RP, the messages are shown as “Sent.” If you execute this command on the VIP console, the IPC messages are shown as “Received.”
-------------------------	---

Examples	The following is sample output of the show route-map ipc command when it is executed on the RP:
-----------------	--

```
Router# show route-map ipc

Route-map RP IPC Config Updates Sent
Name: 4
Match access-list: 2
Match length: 0
Set precedence: 1
Set tos: 0
Set nexthop: 4
Set interface: 0
Set default nexthop: 0
Set default interface: 1
Clean all: 2
```


The following is sample output of the **show route-map ipc** command when it is executed on the VIP:

```
Router# show route-map ipc

Route-map LC IPC Config Updates Received
Name: 4
Match access-list: 2
Match length: 0
Set precedence: 1
Set tos: 0
Set nexthop: 4
Set interface: 0
Set default nexthop: 0
Set default interface: 1
Clean all: 2
```

Table 85 describes the significant fields shown in the display.

Table 85 *show route-map ipc Field Descriptions*

Field	Description
Route-map RP IPC Config Updates Sent	Indicates that IPC messages are being sent from the RP to the VIP.
Name	Number of IPC messages sent about the name of the route map.
Match access-list	Number of IPC messages sent about the access list.
Match length	Number of IPC messages sent about the length to match.
Set precedence	Number of IPC messages sent about the precedence.
Set tos	Number of IPC messages sent about the type of service (ToS).
Set nexthop	Number of IPC messages sent about the next hop.
Set interface	Number of IPC messages sent about the interface.
Set default nexthop	Number of IPC messages sent about the default next hop.
Set default interface	Number of IPC messages sent about the default interface.
Clean all	Number of IPC messages sent about clearing the policy routing configuration from the VIP. When dCEF is disabled and reenabled, the configuration related to policy routing must be removed (cleaned) from the VIP before the new information is downloaded from the RP to the VIP.

Related Commands

Command	Description
set ip next-hop verify-availability	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to that next hop.

show xdr

To display details about eXternal Data Representation (XDR), use the **show xdr** command in user EXEC or privileged EXEC mode.

show xdr {**client** [*client-name* | **all**] [**statistics**] | **linecard** [*linecard-number*] [**internal**] | **multicast-group** | **timers**}

Syntax Description	
client { <i>client-name</i> all }	Displays client basic information or statistics for a client or all clients.
statistics	(Optional) Displays XDR statistics.
linecard	(Line cards only) (Route/Switch Processor (RSP) on Cisco 7500 series and Route Processor (RP) on Cisco 10000 series) Displays XDR information for all XDR line card peer instances or the specified XDR line card peer instance.
<i>linecard-number</i>	(Optional) Specifies the line card slot number.
internal	(Optional) (RSP only) Displays internal information.
multicast-group	Displays XDR multicast groups.
timers	Displays XDR timers.

Command Default XDR details are not displayed.

Command Modes User EXEC (>)
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 This command is available only on distributed platforms (such as the Cisco 7500 series) and on the Cisco 10000 series routers.

Examples The following example shows how to display XDR information for all clients:

```
Router# show xdr client all
```

```
XDR Interrupt P(0) flag:1 decode:0x413B9804 pull:0x413B9AE8 context:8
XDR Process Pri(1) flag:1 decode:0x413B99A0 pull:0x413B9D3C context:6
FIBHWIDB broker(2) flag:1 decode:0x0 pull:0x413A7B7C context:2
```

```

FIBIDB broker (3) flag:1 decode:0x0 pull:0x413A844C context:2
FIBHWIDB Subblo(4) flag:1 decode:0x0 pull:0x413A8E20 context:2
FIBIDB Subblock(5) flag:1 decode:0x0 pull:0x413A97DC context:2
XDR High Queue (6) flag:3 decode:0x4031AFC pull:0x4031B934 context:1
Adjacency updat(7) flag:1 decode:0x413B266C pull:0x413B261C context:2
XDR Medium Queue(8) flag:3 decode:0x4031B004 pull:0x4031B95C context:1
IPv4 table brok(9) flag:1 decode:0x0 pull:0x413B21F0 context:6
IPv6 table brok(10) flag:1 decode:0x0 pull:0x413ECA90 context:6
XDR Low Queue (11) flag:3 decode:0x4031B00C pull:0x4031B984 context:1
MFI RP Pull (12) flag:1 decode:0x0 pull:0x413E1174 context:1
Push Client One(13) flag:1 decode:0x413BA300 pull:0x0 context:4
CEF push (14) flag:1 decode:0x413A3D74 pull:0x0 context:124
MFI non-RP Push(15) flag:1 decode:0x413DFA34 pull:0x0 context:4
XDR ping (16) flag:1 decode:0x413BABB4 pull:0x0 context:1

```

The following example shows how to display XDR information for all XDR line card peer instances:

```
Router# show xdr linecard
```

```

XDR slot number 1, status PEER UP
  IPC messages sent 48
  Next sequence number to send 21
  Maximum sequence number expected 36

XDR slot number 2, status PEER UP
  IPC messages sent 52
  Next sequence number to send 31
  Maximum sequence number expected 46

XDR slot number 3, status PEER UP
  IPC messages sent 55
  Next sequence number to send 17
  Maximum sequence number expected 32

```

The following example shows how to display XDR information for the XDR line card peer instance in slot number 1:

```
Router# show xdr linecard 1
```

```

XDR slot number 1, status PEER UP
  IPC messages sent 48
  Next sequence number to send 21
  Maximum sequence number expected 36

```

The following example shows how to display internal XDR information for the XDR line card peer instance in slot number 1:

```
Router# show xdr linecard 1 internal
```

```

XDR slot number 1, status PEER UP
  IPC messages sent 48
  Next sequence number to send 21
  Maximum sequence number expected 36

```

	Tx	bytes	Rx	bytes	
XDR Interrupt Priority:					
	0	0	2391	11955	Window Message
	21	336	0	0	Time Message
	2	8	0	0	Resequenece Message
	0	0	1	6	CEF LC state
XDR Process Priority:					
	0	0	1	3	Registration Signal
	2	10	0	0	CEF running
FIBHWIDB broker :					
	90	33570	0	0	fibhwwidb update

```

FIBIDB broker      :
      80      30960      0      0      fibidb update
FIBIDB Subblock brok:
      10      315      0      0      fibswsb update
Adjacency update   :
      2       6       0      0      Adjacency update me
      3       9       0      0      Adjacency repopulat
IPv4 table broker  :
      16      558      0      0      prefix
      4       24      0      0      epoch
      2       36      0      0      table
      4       44      0      0      multicast prefix
IPv6 table broker  :
      1       18      0      0      table
CEF push           :
      12      72      19     114     repopulation req
      0       0       1      12     isl table update rq
      0       0       1      12     dot1q table updateq
      2      10       0      0      state
      9     452       0      0      control
      1       3       0      0      flow features deace
      1      22       0      0      flow cache config
      1      40       0      0      flow export config
      6     470       0      0      access-list config
      2      10       0      0      access-list delete
      1      12       0      0      route-map
      1      16       0      0      icmp limit
      1       8       0      0      SSM RP to LC commas
XDR ping           :
      3       12      3      12     ping message

```

The following is sample output from the **show xdr multicast-group** command:

```

Router# show xdr multicast-group

0x4300DC00  READY      Window: 15  Linecards: 2
  XDR High Queue  xdrs to push: 0
  XDR Medium Queu xdrs to push: 0
  XDR Low Queue   xdrs to push: 0

0x4414BC60  READY      Window: 15  Linecards: 1
  XDR High Queue  xdrs to push: 0
  XDR Medium Queu xdrs to push: 0
  XDR Low Queue   xdrs to push: 0

0x44159420  READY      Window: 15  Linecards: 3
  XDR High Queue  xdrs to push: 0
  XDR Medium Queu xdrs to push: 0
  XDR Low Queue   xdrs to push: 0

```

The following is sample output from the **show xdr timers** command:

```

Router# show xdr timers

XDR multicast timers
  Expiration  Type
  |           0.000 (parent)

XDR RP ping timers
  Expiration  Type
  |           0.000 (parent)

XDR RP timers
  Expiration  Type

```

```

|      1:19.236  (parent)
|      1:19.236   Sending Time
|      4:59.236   Keepalive timer slot: 2
|      4:59.236   Keepalive timer slot: 1
|      4:59.248   Keepalive timer slot: 3

```

Cisco 10000 Series Router Examples

The following example shows how to display XDR information for all clients:

```
Router# show xdr client all
```

```

XDR Interrupt P(0) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR Process Pri(1) flag:RP|ISSU aware
  ISSU capable slot(s): 1
FIBHWIDB broker(2) flag:RP|ISSU aware
  ISSU capable slot(s): 1
FIBIDB broker  (3) flag:RP|ISSU aware
  ISSU capable slot(s): 1
FIBHWIDB Subblo(4) flag:RP|ISSU aware
  ISSU capable slot(s): 1
FIBIDB Subblock(5) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR High Queue (6) flag:RP|LC
Adjacency updat(7) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR Medium Queu(8) flag:RP|LC
IPv4 table brok(9) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR Low Queue  (11) flag:RP|LC
MFI Pull        (12) flag:RP|ISSU aware
  ISSU capable slot(s): 1
Push Client One(13) flag:RP
CEF push        (14) flag:RP|ISSU aware
  ISSU capable slot(s): 1
MFI Push        (15) flag:RP|ISSU aware
  ISSU capable slot(s): 1
XDR ping        (16) flag:RP
MPLS Embedded M(17) flag:RP

```

The following example shows how to display XDR information for all XDR line card peer instances:

```
Router# show xdr linecard
```

```

XDR slot number 1, status  PEER UP
  IPC messages sent 569
  This is the secondary RP
  Next sequence number to send      116
  Maximum sequence number expected 160
  ISSU state: Nego done, version 2, mtu 7, sid 31

```

The following example shows how to display XDR information for the XDR line card peer instance in slot number 1:

```
Router# show xdr linecard 1
```

```

XDR slot number 1, status  PEER UP
  IPC messages sent 570
  This is the secondary RP
  Next sequence number to send      116
  Maximum sequence number expected 160
  ISSU state: Nego done, version 2, mtu 7, sid 31

```

The following example shows how to display internal XDR information for the XDR line card peer instance in slot number 1:

Router# **show xdr linecard 1 internal**

```

XDR slot number 1, status  PEER UP
IPC maximum mtu  1478
IPC messages sent 570
This is the secondary RP
Next sequence number to send      116
Maximum sequence number expected 160
ISSU state: Nego done, version 2, mtu 7, sid 31

```

	Tx	bytes	Rx	bytes	
XDR Interrupt Priori:					
	0	0	10427	52135	Window Message
	87	1392	0	0	Time Message
	1	4	0	0	Resequence Message
	19	444	11	264	ISSU nego
XDR Process Priority:					
	17	51	11	33	Reg Signal
	1	2	0	0	CEF running
	0	0	1	4	CEF reload request
	15	348	9	216	ISSU nego
FIBHWIDB broker :					
	32	3588	0	0	fibhwidb update
	7	156	5	120	ISSU nego
FIBIDB broker :					
	49	6429	0	0	fibidb update
	7	156	5	120	ISSU nego
FIBHWIDB Subblock br:					
	7	156	5	120	ISSU nego
FIBIDB Subblock brok:					
	41	1533	0	0	fibswsb update
	13	300	8	192	ISSU nego
Adjacency update :					
	62	3089	0	0	adj update
	4	8	0	0	adj epoch
	17	396	10	240	ISSU nego
IPv4 table broker :					
	285	28557	0	0	prefix
	8	48	0	0	epoch
	5	78	0	0	table
	5	55	0	0	multicast prefix
	45	1068	24	576	ISSU nego
MFI Pull :					
	12	456	0	0	pull update
	75	1788	39	936	ISSU nego
CEF push :					
	8	48	14	84	repopulation req
	5	10	0	0	state
	12	816	0	0	control
	2	0	0	0	mpls_access-list delete
	2	32	0	0	icmp limit
	9	204	6	144	ISSU nego
MFI Push :					
	3	101	0	0	service reply
	2	34	0	0	client request
	0	0	4	106	service request
	2	16	0	0	enable/redist redistribution
client					
	153	3660	78	1872	ISSU nego
XDR ping :					
	6	24	6	24	ping message

Related Commands

Command	Description
show cef broker	Displays Cisco Express Forwarding information related to a selected update broker.

snmp mib cef throttling-interval

To set the throttling interval for the CEF-MIB inconsistency notifications, use the **snmp mib cef throttling-interval** command in global configuration mode. To remove the throttling interval, use the **no** form of this command.

snmp mib cef throttling-interval *seconds*

no snmp mib cef throttling-interval *seconds*

Syntax Description

<i>seconds</i>	The time to allow before an inconsistency notification is sent during the process of updating forwarding information from the Routing Information Base (RIB) to the Route Processor (RP) and the line card databases. The valid values are from 0 to 3600 seconds.
----------------	--

Command Default

Throttling is disabled by default (throttling interval is set to 0 seconds).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
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 this command in conjunction with the **snmp-server enable traps cef inconsistency** command to set the time that elapsed between the occurrence of a Cisco Express Forwarding database inconsistencies and the time when you want to receive an inconsistency notification.

If you set the throttling interval to 0 seconds, throttling is disabled.

Examples

The following example shows how to set the throttling interval for CEF-MIB inconsistency notification to 300 seconds:

```
configure terminal
!
snmp-server enable traps cef inconsistency
snmp mib cef throttling-interval 300
```


Related Commands

Command	Description
snmp-server enable traps cef	Enables CEF-MIB notifications that correspond to Cisco Express Forwarding events.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps cef

To enable Cisco Express Forwarding support of Simple Network Management Protocol (SNMP) notifications on a network management system (NMS), use the **snmp-server enable traps cef** command in global configuration mode. To disable Cisco Express Forwarding support of SNMP notifications, use the **no** form of this command.

snmp-server enable traps cef [**peer-state-change**] [**resource-failure**] [**inconsistency**]
[**peer-fib-state-change**]

no snmp-server enable traps cef [**peer-state-change**] [**resource-failure**] [**inconsistency**]
[**peer-fib-state-change**]

Syntax Description

peer-state-change	(Optional) Enables the sending of CEF-MIB SNMP notifications for changes in the operational state of Cisco Express Forwarding peers.
resource-failure	(Optional) Enables the sending of CEF-MIB SNMP notifications for resource failures that affect Cisco Express Forwarding operations.
inconsistency	(Optional) Enables the sending of CEF-MIB SNMP notifications for inconsistencies that occur when routing information is updated from the Routing Information Base (RIB) to the Cisco Express Forwarding Forwarding Information Base (FIB) on the Route Processor (RP) and to the Cisco Express Forwarding FIB on the line cards.
peer-fib-state-change	(Optional) Enables the sending of CEF-MIB SNMP notifications for changes in the operational state of the Cisco Express Forwarding peer FIB.

Command Default

All CEF-MIB notifications are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
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

You can use this command to enable CEF-MIB SNMP notifications that correspond to specific Cisco Express Forwarding events. To send the notifications to an NMS or host system, you must configure the **snmp-server host** command with the **cef** keyword.

You can enable all CEF-MIB SNMP notifications if you enter the **snmp-server enable traps cef** command without entering an optional keyword.

Examples

The following example shows how to enable a router to send Cisco Express Forwarding peer state changes and forwarding inconsistencies as informs to the NMS with IP address 10.56.125.47 and to use the community string defined as public:

```
configure terminal
!
snmp-server enable traps cef peer-state-change inconsistency
snmp-server host 10.56.125.47 informs version 2c public
```

Related Commands

Command	Description
snmp-server community	Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

no snmp-server host {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

Syntax Description

<i>hostname</i>	Name of the host. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.
<i>ip-address</i>	IP address or IPv6 address of the SNMP notification host.
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications.
<i>vrf-name</i>	(Optional) VPN VRF instance used to send SNMP notifications.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
informs	(Optional) Specifies that notifications should be sent as informs.
version	(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. If you use the version keyword, one of the following keywords must be specified: 1—SNMPv1. 2c—SNMPv2C. 3—SNMPv3. The most secure model because it allows packet encryption with the priv keyword. The default is noauth. One of the following three optional security level keywords can follow the 3 keyword: auth—Enables message digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. noauth—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. priv—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
<i>community-string</i>	Password-like community string sent with the notification operation. Note You can set this string using the snmp-server host command by itself, but Cisco recommends that you define the string using the snmp-server community command prior to using the snmp-server host command. Note The “at” sign (@) is used for delimiting the context information.

udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an NMS host.
<i>port</i>	(Optional) User Datagram Protocol (UDP) port number of the NMS host. The default is 162.
<i>notification-type</i>	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. You can specify more than one of the following notification types: Note The available notification types differ based on the platform and Cisco IOS release. For a complete list of available notification types, use the question mark (?) online help function. • atm—Sends ATM notifications. • auth-framework—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB notifications. • bgp—Sends Border Gateway Protocol (BGP) state change notifications. • bridge—Sends SNMP STP Bridge MIB notifications. • bstun—Sends Block Serial Tunnel (BSTUN) event notifications. • bulkstat—Sends Data-Collection-MIB notifications. • c6kxbar—Sends SNMP crossbar notifications. • callhome—Sends Call Home MIB notifications. • calltracker—Sends Call Tracker call-start/call-end notifications. • casa—Sends Cisco Appliance Services Architecture (CASA) event notifications. • cef —Sends notifications related to Cisco Express Forwarding. • chassis—Sends SNMP chassis notifications. • config—Sends configuration change notifications. • config-copy—Sends SNMP config-copy notifications. • config-ctid—Sends SNMP config-ctid notifications. • cpu—Sends CPU-related notifications. • csg—Sends SNMP Content Services Gateway (CSG) notifications. • dhcp-snooping—Sends Dynamic Host Configuration Protocol (DHCP) snooping MIB notifications. • director—Sends notifications related to DistributedDirector. • dls—Sends data-link switching (DLSw) notifications. • dot1x—Sends 802.1X notifications. • ds1—Sends SNMP digital signal 1 (DS1) notifications. • dspu—Sends downstream physical unit (DSPU) notifications. • eigrp—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.

-
- **energywise**—Sends SNMP energywise notifications.
 - **entity**—Sends Entity MIB modification notifications.
 - **entity-diag**—Sends SNMP entity diagnostic MIB notifications.
 - **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
 - **errdisable**—Sends error disable notifications.
 - **ethernet-cfm**—Sends SNMP Ethernet Connectivity Fault Management (CFM) notifications.
 - **event-manager**—Sends SNMP Embedded Event Manager notifications.
 - **flash**—Sends flash media insertion and removal notifications.
 - **flexlinks**—Sends FLEX links notifications.
 - **flowmon**—Sends flow monitoring notifications.
 - **frame-relay**—Sends Frame Relay notifications.
 - **fru-ctrl**—Sends entity field-replaceable unit (FRU) control notifications.
 - **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
 - **ipmulticast**—Sends IP multicast notifications.
 - **iplocalpool**—Sends IP local pool notifications.
 - **ipmobile**—Sends Mobile IP notifications.
 - **ipsec**—Sends IP Security (IPsec) notifications.
 - **isakmp**—Sends SNMP Internet Security Association and Key Management Protocol (ISAKMP) notifications.
 - **isdn**—Sends ISDN notifications.
 - **l2tc**—Sends SNMP Layer 2 (L2) tunnel configuration notifications.
 - **l2tun-pseudowire-status**—Sends pseudowire state change notifications.
 - **l2tun-session**—Sends Layer 2 tunneling session notifications.
 - **license**—Sends licensing notifications as traps or informs.
 - **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
 - **mac-notification**—Sends SNMP MAC notifications.
 - **memory**—Sends memory pool and memory buffer pool notifications.
 - **module**—Sends SNMP module notifications.
 - **module-auto-shutdown**—Sends SNMP module auto shutdown MIB notifications.
 - **mpls-fast-reroute**—Sends SNMP MPLS traffic engineering fast reroute notifications.
-

- **mpls-ldp**—Sends Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **msdp**—Sends SNMP Multicast Source Discovery Protocol (MSDP) notifications.
- **mvpn**—Sends multicast Virtual Private Network notifications.
- **nhrp**—Sends Next Hop Resolution Protocol (NHRP) notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **port-security**—Sends SNMP port-security notifications.
- **power-ethernet**—Sends SNMP power Ethernet notifications.
- **pw-vc**—Sends SNMP pseudowire (PW) virtual circuit (VC) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **rf**—Sends SNMP Redundancy Framework (RF) MIB notifications.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **slb**—Sends SNMP server load balancer (SLB) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC 2233 compliant link up/down notifications, you should use the **snmp server link trap** command.

- **sonet**—Sends SNMP Synchronous Optical Networking (SONET) notifications.
- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stpx**—Sends SNMP CISCO-STP-EXTENSIONS-MIB (STPX-MIB) notifications.
- **stun**—Sends serial tunnel (STUN) notifications.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.

- **udp-port**—Sends the notification host's UDP port number.
- **vlan-mac-limit**—Sends SNMP L2 control VLAN MAC limit notifications.
- **vlancreate**—Sends SNMP VLAN created notifications.
- **vlandelete**—Sends SNMP VLAN deleted notifications.
- **voice**—Sends SNMP voice traps.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vswitch**—Sends SNMP virtual switch notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) notifications.
- **x25**—Sends X.25 event notifications.

Command Default

This command is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	This command was modified. The 3 , auth , noauth , and priv keywords were added as part of the SNMPv3 Support feature. The hsrp and voice notification-type keywords were added.
12.1(3)T	This command was modified. The calltracker notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	This command was modified. The vrf vrf-name keyword and argument combination was added. The ipmobile notification-type keyword was added. Support for the vsimaster notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	This command was modified. The pim and ipsec notification-type keywords were added.
12.2(8)T	This command was modified. The mpls-traffic-eng and director notification-type keywords were added.
12.2(13)T	This command was modified. The srp and mpls-ldp notification-type keywords were added.
12.3(2)T	This command was modified. The flash and l2tun-session notification-type keywords were added.
12.3(4)T	This command was modified. The cpu , memory , and ospf notification-type keywords were added.
12.3(8)T	This command was modified. The iplocalpool notification-type keyword was added for the Cisco 7200 and 7301 series routers.

Release	Modification
12.3(11)T	This command was modified. The vrrp keyword was added.
12.3(14)T	This command was modified. Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument. The eigrp notification-type keyword was added.
12.4(20)T	This command was modified. The license notification-type keyword was added.
Cisco IOS Release 12.0S	
12.0(17)ST	This command was modified. The mpls-traffic-eng notification-type keyword was added.
12.0(21)ST	This command was modified. The mpls-ldp notification-type keyword was added.
12.0(22)S	This command was modified. All features in the Cisco IOS Release 12.0ST train were integrated into Cisco IOS Release 12.0(22)S. The mpls-vpn notification-type keyword was added.
12.0(23)S	This command was modified. The l2tun-session notification-type keyword was added.
12.0(26)S	This command was modified. The memory notification-type keyword was added.
12.0(27)S	This command was modified. Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument. The vrf vrf-name keyword and argument combination was added to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	This command was modified. The l2tun-pseudowire-status notification-type keyword was added.
Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	This command was modified. The cpu and memory notification-type keywords were added.
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(31)SB2	This command was modified. The cef notification-type keyword was added.
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.
12.2(33)SXI4	This command was modified. The dhcp-snooping and errdisable notification-type keywords were added.
12.2(33)SRE	This command was modified. The automatic insertion of the snmp-server community command into the configuration, along with the community string specified in the snmp-server host command, was changed. The snmp-server community command must be manually configured.
Cisco IOS Release 15.0	
15.0(1)S	This command was modified. The flowmon notification-type keyword was added.

Release	Modification
15.0(1)M	This command was modified. The nhrp notification-type keyword was added. The automatic insertion of the snmp-server community command into the configuration, along with the community string specified in the snmp-server host command, is changed. The snmp-server community command has to be manually configured.
Cisco IOS XE	
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.



Note

In Cisco IOS Release 12.0(3) to 12.2(33)SRD, if a community string was not defined using the **snmp-server community** command prior to using the **snmp-server host** command, the default form of the **snmp-server community** command was automatically inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** was the same as that specified in the **snmp-server host** command. However, in Cisco IOS Release 12.2(33)SRE and later releases, you must manually configure the **snmp-server community** command.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others are enabled by a different command. For example, the **linkUpDown** notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of a notification-type options depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command **help ?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a user so data is stored using the VPN.

In the case of the NMS sending the query having a correct SNMP community but that does not have a read or a write view, the SNMP agent returns the following error values:

- For a get or a getnext query, returns GEN_ERROR for SNMPv1 and AUTHORIZATION_ERROR for SNMPv2C.
- For a set query, returns NO_ACCESS_ERROR.

Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the command-line interface (CLI) interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. [Table 86](#) maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 86 *SNMP-server enable traps Commands and Corresponding Notification Keywords*

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	l2tun-session
snmp-server enable traps mpls ldp	mpls-ldp
snmp-server enable traps mpls traffic-eng ¹	mpls-traffic-eng
snmp-server enable traps mpls vpn	mpls-vpn

1. See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 192.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

**Note**

The “at” sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community@VLAN-ID* (for example, public@100), where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a specified host named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 192.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 192.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to example.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host example.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 192.40.3.130 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all NHRP traps to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 192.40.3.130 traps version 2c public nhrp
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP trap that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

switchover pxf restart

To configure the number of parallel express forwarding (PXF) restarts that are allowed before a switchover to a redundant Performance Routing Engine (PRE) module, use the **switchover pxf restart** command in redundancy configuration (main-cpu) mode. To disable switchovers due to PXF restarts, use the **no** form of this command.

switchover pxf restart *number-of-restarts time-period*

no switchover pxf restart

Syntax Description

<i>number-of-restarts</i>	The number of PXF restarts that are allowed within the specified time period. If the PXF processors restart this many times within the given time period, the router switches over to the redundant PRE module. The valid range is 1 to 25. The default is 2 PXF restarts within 5 hours.
<i>time-period</i>	Time period, in hours, that PXF restart counts are monitored. The valid range is 0 to 120 hours.
Note A value of 0 specifies that a switchover occurs on the configured <i>number-of-restarts</i> regardless of the time period.	

Command Default

If this command is not configured, the default is 2 PXF restarts within 5 hours.

Command Modes

Redundancy configuration, main-cpu mode (config-r-mc)

Command History

Release	Modification
12.2(15)BC2	This command was introduced on the Cisco uBR10012 router.
12.3(7)	This command was introduced on the Cisco 10000 series router and integrated into Cisco IOS Release 12.3(7).
12.2SB	This command was integrated into Cisco IOS Release 12.2SB.

Usage Guidelines

The startup and running configurations of the standby PRE are synchronized with the active PRE, ensuring the fastest possible cut-over time if the active PRE fails. A second switchover is prevented for 2 hours if a PXF restart occurs on the new active PRE.

A PXF restart following a PXF fault may restore service more quickly when the features in use are not configured for nonstop forwarding with stateful switchover (NSF/SSO), or when SSO mode is not configured on the router. Conversely, a PRE switchover in response to a PXF restart may restore service more quickly when NSF/SSO is configured on the router and all configured features support NSF/SSO.

When a switchover occurs because of repeated PXF restarts, the router displays the following system message:

```
C10KEVENTMGR-3-PXF_FAIL_SWITCHOVER: Multiple PXF failures, switchover to redundant PRE initiated.
```

Examples

The following example shows how to configure the router so that if five PXF restarts occur within a one-hour period, the router initiates a switchover to the redundant PRE module.

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-r-mc)# switchover pxf restart 5 1
```

Related Commands

Command	Description
main-cpu	Enters main-cpu redundancy configuration mode to configure the synchronization of the active and standby PRE modules.
redundancy	Configures the synchronization of system files between the active and standby PRE modules.
redundancy force-failover main-cpu	Forces a manual switchover between the active and standby PRE modules.
show redundancy	Displays the current redundancy status.

test cef table consistency

To test the Cisco Express Forwarding Forwarding Information Base (FIB) for prefix consistency, use the **test cef table consistency** command in privilege EXEC mode.

test cef table consistency [detail]

Syntax Description	detail	(Optional) Displays detailed information about the consistency of prefixes in the Cisco Express Forwarding FIB table.
---------------------------	---------------	---

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

Command History	Release	Modification
	12.2(25)S	This command was introduced. This command replaces the show ip cef inconsistency command .
	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

This command displays recorded Cisco Express Forwarding consistency records found by the lc-detect, scan-rib-ios, scan-ios-rib, scan-lc-rp, and scan-rp-lc detection mechanisms. The scan-lc-rp and scan-rp-lc detection mechanisms are available only on routers with line cards.

You can configure the Cisco Express Forwarding prefix consistency-detection mechanisms using the **cef table consistency-check** command.

Examples

The following is sample output from the **test cef table consistency** command:

```
Router# test cef table consistency

full-scan-rib-ios: Checking IPv4 RIB to FIB consistency
full-scan-ios-rib: Checking IPv4 FIB to RIB consistency
No IPv4 inconsistencies found, check took 00:00:00.000
```

The following is sample output from the **test cef table consistency detail** command:

```
Router# test cef table consistency detail

full-scan-rib-ios: Checking IPv4 RIB to FIB consistency
full-scan-rib-ios: FIB checked 12 prefixes, and found 0 missing.
full-scan-ios-rib: Checking IPv4 FIB to RIB consistency
full-scan-ios-rib: Checked 12 FIB prefixes in 1 pass, and found 0 extra.
full-scan-rp-lc: Sent 26 IPv4 prefixes to linecards in 1 pass
full-scan-rp-lc: Initiated IPv4 FIB check on linecards..4..1..0..
full-scan-rp-lc: FIB IPv4 check completed on linecards..1..0..4..
full-scan-rp-lc: Linecard 4 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 1 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
```



```

full-scan-rp-lc: Linecard 0 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
full-scan-rib-ios: Checking IPv6 RIB to FIB consistency
full-scan-rib-ios: FIB checked 16 prefixes, and found 5 missing.
full-scan-ios-rib: Checking IPv6 FIB to RIB consistency
full-scan-ios-rib: Checked 11 FIB prefixes in 1 pass, and found 0 extra.
full-scan-rp-lc: Sent 11 IPv6 prefixes to linecards in 1 pass
full-scan-rp-lc: Initiated IPv6 FIB check on linecards..4..1..0..
full-scan-rp-lc: FIB IPv6 check completed on linecards..1..4..0..
full-scan-rp-lc: Linecard 4 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 1 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 0 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
No IPv4 inconsistencies found, check took 00:00:01.444
Warning: 5 IPv6 inconsistencies found, check took 00:00:01.240

```

Table 87 describes the significant fields shown in the display.

Table 87 *test cef consistency detail Field Descriptions*

Field	Description
FIB checked 12 prefixes, and found 0 missing	The scan-rib-ios consistency checker checked 12 prefixes in the FIB against the FIB and found 0 missing.
Checked 12 FIB prefixes in 1 pass, and found 0 extra.	The scan-ios-rib consistency checker checked 12 prefixes in the RIB and found no extra prefixes in one pass.
Linecard 4 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.	The scan-rp-lc consistency checker found no inconsistencies on line card 4 after checking 26 IPv4 prefixes.

Related Commands

Command	Description
cef table consistency check	Enables Cisco Express Forwarding table consistency checker types and parameters.