# IP Switching Cisco Express Forwarding Configuration Guide, Cisco IOS XE Gibraltar 16.10.x

**First Published:** 2019-10-01

**Last Modified:** 2023-10-25

**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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

# CONTENTS

CHAPTER 1

# Read Me First

### Important Information

**Note** For CUBE feature support information in Cisco IOS XE Bengaluru 17.6.1a and later releases, see Cisco Unified Border Element IOS-XE Configuration Guide.

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

### Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

### Related References

- Cisco IOS Command References, All Releases

### Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

# Short Description

CHAPTER 2

# CEF Overview

This module contains an overview of the Cisco Express Forwarding feature. Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

# Information About CEF

## Cisco Platform Support for Central CEF and dCEF

Cisco Express Forwarding is enabled by default on most Cisco platforms running Cisco IOS software Release12.0 or later. When Cisco Express Forwarding is enabled on a router, the Route Processor (RP) performs the express forwarding.

To find out if Cisco Express Forwarding is enabled on your platform, enter the **show ip cef**command. If Cisco Express Forwarding is enabled, you receive output that looks like this:

```
Router# show ip cef
Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet6/1
[...]
```

If Cisco Express Forwarding is not enabled on your platform, the output for the **show ip cef**command looks like this:

```
Router# show ip cef
%CEF not running
```

Distributed Cisco Express Forwarding is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When distributed Cisco Express Forwarding is enabled on your platform, the line cards perform the express forwarding.

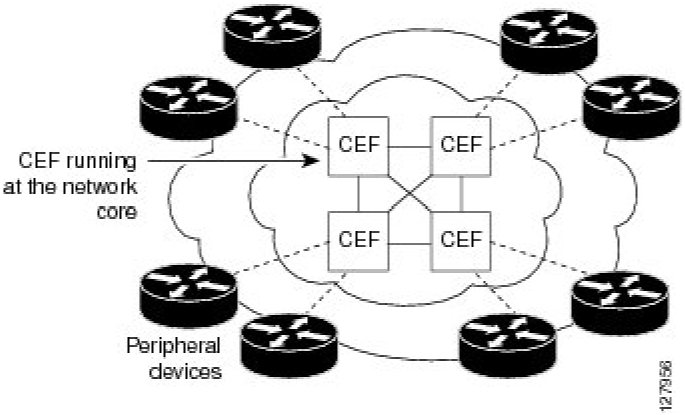
If Cisco Express Forwarding is not enabled on your platform, use the **ip cef**command to enable (central) Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

# Cisco Express Forwarding Benefits

- Improved performance--Cisco Express Forwarding is less CPU-intensive than fast switching route caching. As a result, more CPU processing power can be dedicated to Layer 3 services such as quality of service (QoS) and encryption.
- Scalability--Cisco Express Forwarding offers full switching capacity at each line card when distributed Cisco Express Forwarding mode is active. Distributed Cisco Express Forwarding is a distributed switching mechanism that scales linearly with the number of interface cards and the bandwidth installed in the router.
- Resilience--Cisco Express Forwarding offers an unprecedented level of switching consistency and stability in large dynamic networks. In dynamic networks, fast-switched cache entries are frequently invalidated by routing changes. These changes can cause traffic to be process-switched through use of the routing table, rather than fast switched through use of the route cache. Because the forwarding information base (FIB) lookup table contains all known routes that exist in the routing table, it eliminates the need for route cache maintenance and the steps involved with fast-switch or process-switch forwarding. Cisco Express Forwarding can switch traffic more efficiently than typical demand caching schemes.

You can use Cisco Express Forwarding in any part of a network. For example, the figure below shows Cisco Express Forwarding being run on routers at aggregation points at the core of a network where traffic levels are high and performance is critical.

*Figure 1: Cisco Express Forwarding Example*



Cisco Express Forwarding in platforms at the network core provides the performance and scalability that networks need to respond to continued growth and steadily increasing network traffic. Cisco Express Forwarding is a distributed switching mechanism that scales linearly with the number of interface cards and the bandwidth installed in the router.

# Media Supported by CEF

Cisco Express Forwarding supports the following media:

- ATM/AAL5snap, ATM/AAL5mux, and ATM/AAL5nlpid
- Ethernet
- FDDI
- Frame Relay
- High-Level Data Link Control (HDLC)
- PPP
- Spatial Reuse Protocol (SRP)
- Token Ring
- Tunnels

# Main Components of CEF

Information conventionally stored in a route cache is stored in several data structures for Cisco Express Forwarding switching. The data structures provide optimized lookup for efficient packet forwarding. The two main components of Cisco Express Forwarding operation are the forwarding information base (FIB) and the adjacency tables.

The FIB is conceptually similar to a routing table or information base. A router uses this lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The FIB is updated when changes occur in the network and contains all routes known at the time. For more information, see the *FIB Overview* section.

Adjacency tables maintain Layer 2 next-hop addresses for all FIB entries. For more information, see the *CEF Adjacency Tables Overview* section.

This separation of the reachability information (in the Cisco Express Forwarding table) and the forwarding information (in the adjacency table), provides a number of benefits:

- The adjacency table can be built separately from the Cisco Express Forwarding table, allowing both to be built without any packets being process-switched.
- The MAC header rewrite used to forward a packet is not stored in cache entries, so changes in a MAC header rewrite string do not require validation of cache entries.

# FIB Overview

Cisco Express Forwarding uses a forwarding information base (FIB) to make IP destination prefix-based switching decisions.

The FIB contains the prefixes from the IP routing table structured in a way that is optimized for forwarding. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.

Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for the route cache maintenance that is associated with switching paths such as those used in fast switching and optimum switching.

## CEF FIB and Load Balancing

Several paths can lead to a destination prefix. This occurs, for example, when a router is configured for simultaneous load balancing and redundancy. For each resolved path, the FIB contains a pointer for the adjacency corresponding to the next hop interface for that path.

**Note** Layer 3 Equal-cost multi path (ECMP) load balancing is based on source IP address, destination IP address, source port, destination port, and layer 4 protocol. Fragmented packets will be treated on two different links based on the algorithm calculated using these parameters. Any changes in one of these parameters will result in load balancing.

# CEF Adjacency Tables Overview

A node is said to be adjacent to another node if the node can be reached with a single hop across a link layer (Layer 2). Cisco Express Forwarding stores forwarding information (outbound interface and MAC header rewrite) for adjacent nodes in a data structure called the adjacency table. Cisco Express Forwarding uses adjacency tables to prepend Layer 2 addressing information to packets. The adjacency tables maintain Layer 2 next-hop addresses for all FIB entries.

The following sections provide additional information about adjacencies:

## Adjacency Discovery

Each adjacency table is populated as adjacencies are discovered. Adjacencies are added to the table through indirect manual configuration or dynamically--discovered through a mechanism like Address Resolution Protocol (ARP). Adjacencies can also be added through the use of a routing protocol, such as Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF), which forms neighbor relationships. Each time an adjacency entry is created, a link-layer header for that adjacent node is computed and stored in the adjacency table.

The adjacency information is subsequently used for encapsulation during Cisco Express Forwarding switching of packets.

## Adjacency Types That Require Special Handling

In addition to adjacencies associated with next-hop interfaces (host-route adjacencies), other types of adjacencies are used to expedite switching when certain exception conditions exist. Prefixes requiring exception processing or special handling are cached with one of the special adjacencies listed in the table below.

***Table 1: Adjacency Types That Require Special Handling***

| Packets of This Adjacency Type | Receive This Processing |
|---|---|
| Null adjacency | Packets destined for a Null0 interface are dropped. Null adjacency can be used as an effective form of access filtering. |
| Glean adjacency | When a device is connected to a multiaccess medium, the FIB table on the device maintains a prefix for the subnet rather than for the individual host prefixes. The subnet prefix points to a glean adjacency. A glean adjacency entry indicates that a particular next hop should be directly connected, but there is no MAC header rewrite information available. When the device needs to forward packets to a specific host on a subnet, Cisco Express Forwarding requests an ARP entry for the specific prefix, ARP sends the MAC address, and the adjacency entry for the host is built. |
| Punt adjacency | The device forwards packets requiring special handling or packets sent by features not yet supported in CEF switching paths to the next higher switching level for handling. |
| Discard adjacency | The device discards the packets. |
| Drop adjacency | The device drops the packets. |

## Unresolved Adjacency

When a link-layer header is prepended to a packet, the FIB requires the prepended header to point to an adjacency corresponding to the next hop. If an adjacency was created by the FIB and not discovered through a mechanism such as ARP, the Layer 2 addressing information is not known and the adjacency is considered incomplete or unresolved. Once the Layer 2 information is known, the packet is forwarded to the RP, and the adjacency is determined through ARP. Thus, the adjacency is resolved.

# Central CEF Mode Operation

You can use central Cisco Express Forwarding mode when line cards are not available for Cisco Express Forwarding switching, when you need to use features not compatible with distributed Cisco Express Forwarding switching, or when you are running on a nondistributed platform. When central Cisco Express Forwarding mode is enabled, the Cisco Express Forwarding FIB and adjacency tables reside on the RP, and the RP performs the express forwarding.

The figure below shows the relationship between the routing table, the FIB, and the adjacency table during central Cisco Express Forwarding mode operation. The Catalyst switches forward traffic from workgroup LANs to a Cisco 7500 series router on the enterprise backbone running central Cisco Express Forwarding. The RP performs the express forwarding.

# Distributed CEF Mode Operation

For additional scalability, Cisco Express Forwarding runs in the distributed Cisco Express Forwarding form on certain platforms by spreading processing tasks across two or more line cards. When distributed Cisco Express Forwarding mode is enabled, line cards maintain identical copies of the FIB and adjacency tables. The line cards perform the express forwarding between port adapters, relieving the RP of involvement in the switching operation, thus also enhancing system performance.

Distributed Cisco Express Forwarding uses an interprocess communication (IPC) mechanism to ensure synchronization of FIB tables and adjacency tables on the RP and line cards.

The figure below shows the relationship between the RP and line cards when distributed Cisco Express Forwarding mode is active.

In the Cisco 12000 Series Internet Router, shown in the figure above, the line cards perform the switching. In other routers where you can mix various types of cards in the same router, all cards might not support distributed Cisco Express Forwarding. When a line card that does not support distributed Cisco Express Forwarding receives a packet on one of these other routers, the line card forwards the packet to the next higher switching layer (the RP). This structure allows legacy interface processors to exist in the router with newer interface processors.

**Note** The Cisco 12000 Series Internet routers operate only in distributed Cisco Express Forwarding mode.

# CEF Features Enabled by Default

- Per-destination load balancing and the universal load sharing algorithm
- Distributed tunnel switching
- Multipoint generic routing encapsulation (GRE) tunnels

## CEF Distributed Tunnel Switching

Cisco Express Forwarding supports distributed tunnel switching, such as that made possible by generic routing encapsulation (GRE) tunnels. Distributed tunnel switching is enabled automatically when you enable Cisco Express Forwarding or distributed Cisco Express Forwarding. You do not perform any additional tasks to enable distributed tunnel switching once you enable Cisco Express Forwarding or distributed Cisco Express Forwarding.

## CEF-Switched Multipoint GRE Tunnels

The Cisco Express Forwarding-Switched Multipoint GRE Tunnels feature enables Cisco Express Forwarding switching of IP traffic to and from multipoint GRE tunnels. Traffic can be forwarded to a prefix through a tunnel destination when both the prefix and the tunnel destination are specified by the application. GRE creates a virtual point-to-point link to other routers at remote points over an IP internetwork. GRE can encapsulate a wide variety of protocol type packets. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

# Links for the CEF Features

The table below contains links to information about features that you can configure for use with Cisco Express Forwarding or distributed Cisco Express Forwarding operation.

*Table 2: Features to Configure for Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation*

| For Information on This Feature... | See the Following Document... |
|---|---|
| Configuring and verifying basic Cisco Express Forwarding operation | Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks |
| Enabling or disabling Cisco Express Forwarding or distributed Cisco Express Forwarding switching and forwarding | Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding to Customize Switching and Forwarding for Dynamic Networks |
| Changing your load-balancing scheme | Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic |
| Refreshing or rebuilding adjacency or Cisco Express Forwarding tables | Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables |
| Configuring Cisco Express Forwarding consistency checkers | Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards |
| Configuring network accounting for Cisco Express Forwarding | Configuring Cisco Express Forwarding Network Accounting |
| Customizing the display of recorded Cisco Express Forwarding events | Customizing the Display of Recorded Cisco Express Forwarding Events |

# How to Configure CEF

There are no tasks for configuring Cisco Express Forwarding. Cisco Express Forwarding is enabled by default on most Cisco devices running Cisco software.

See the “Related Documents” section for links to configuration information for Cisco Express Forwarding features and services.

# Configuration Examples for CEF

There are no configuration examples for the Cisco Express Forwarding.

See the “Related Documents” section for links to configuration information for Cisco Express Forwarding features and services.

# Where to Go Next

See the "Related Documents" section for links to configuration information for Cisco Express Forwarding features and services.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples. | *Cisco IOS IP Switching Command Reference* |
| Tasks for verifying Cisco Express Forwarding information on your router | Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks |
| Tasks for enabling or disabling Cisco Express Forwarding or distributed Cisco Express Forwarding | Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding to Customize Switching and Forwarding for Dynamic Networks |
| Tasks for configuring a load-balancing scheme for Cisco Express Forwarding | Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic |
| Tasks for configuring Cisco Express Forwarding consistency checkers | Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards |
| Tasks for configuring epochs for Cisco Express Forwarding tables | Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables |
| Tasks for configuring and verifying Cisco Express Forwarding network accounting | Configuring Cisco Express Forwarding Network Accounting |
| Tasks for customizing the display of recorded Cisco Express Forwarding events | Customizing the Display of Recorded Cisco Express Forwarding Events |

| Related Topic | Document Title |
|---|---|
| Verification steps for Cisco Express Forwarding switching | How to Verify Cisco Express Forwarding Switching |
| Troubleshooting tips for incomplete adjacencies | Troubleshooting Incomplete Adjacencies with CEF |
| Description and use of the Cisco Express Forwarding consistency checkers available for the Cisco 7500 and 12000 series routers | Troubleshooting Prefix Inconsistencies with Cisco Express Forwarding |
| Information about troubleshooting Cisco Express Forwarding routing loops and suboptimal routing | Troubleshooting Cisco Express Forwarding Routing Loops |
| Causes of common Cisco Express Forwarding-related error messages on platforms running distributed Cisco Express Forwarding switching (Cisco 7500 series routers and Cisco 12000 Series Internet routers) and how to troubleshoot them | Troubleshooting Cisco Express Forwarding-Related Error Messages |
| Explanation of and troubleshooting information for the Cisco IOS software implementation of Layer 3 load balancing across multiple parallel links when Cisco Express Forwarding is used | Troubleshooting Load Balancing Over Parallel Links Using Cisco Express Forwarding |
| Troubleshooting guide for unicast IP routing on Catalyst 6500/6000 switches with Supervisor Engine 2, Policy Feature Card 2 (PFC2), or Multilayer Switch Feature Card 2 (MSFC2) | Troubleshoot Unicast IP Routing Involving CEF on Catalyst 6500/6000 Series Switches with a Supervisor Engine 2 and Running CatOS System Software |
| QoS features that require Cisco Express Forwarding | When Is CEF Required for Quality of Service |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| RFC 1701 | *Generic Route Encapsulation (GRE)* |
| RFC 2784 | *Generic Routing Encapsulation (GRE)* |
| RFC 2890 | *Key and Sequence Number Extensions to GRE* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for CEF

*Table 3: Feature Information for Cisco Express Forwarding Overview*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| Cisco Express Forwarding-Switched Multipoint GRE Tunnels | 12.2(8)T | This feature enables Cisco Express Forwarding switching of IP traffic to and from multipoint GRE tunnels. Prior to the introduction of this feature, only process switching was available for multipoint GRE tunnels. |
| CEF Support for IP Routing between IEEE 802.1Q vLANs | Cisco IOS XE Release 2.1 15.0(1)S | This feature was introduced on Cisco ASR 1000 Series Routers.<br>This feature was integrated into Cisco IOS Release 15.0(1)S. |

# Glossary

**adjacency** --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

**Cisco Express Forwarding** --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco

Express Forwarding enables a Route Processor to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

**distributed Cisco Express Forwarding** --A mode of Cisco Express Forwarding operation in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

**FIB** --forwarding information base. A component of Cisco Express Forwarding that is conceptually similar to a routing table or information base. The router uses the FIB lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

**GRE** --generic routing encapsulation. A tunneling protocol developed by Cisco that enables encapsulation of a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows the expansion of a network across a single-protocol backbone environment.

**IPC** --interprocess communication. The mechanism that enables the distribution of Cisco Express Forwarding tables from the Route Switch Processor (RSP) to the line card when the router is operating in distributed Cisco Express Forwarding mode.

**label disposition** --The removal of Multiprotocol Label Switching (MPLS) headers at the edge of a network. In MPLS label disposition, packets arrive on a router as MPLS packets and, with the headers removed, are transmitted as IP packets.

**label imposition** --The action of putting a label on a packet.

**LER** --label edge router. A router that performs label imposition.

**LFIB** --label forwarding information base. The data structure used by switching functions to switch labeled packets.

**LIB** --label information base. A database used by a label switch router (LSR) to store labels learned from other LSRs, as well as labels assigned by the local LSR.

**line card** --A general term for an interface processor that can be used in various Cisco products. For example, a Versatile Interface Processor (VIP) is a line card for the Cisco 7500 series router.

**LSP** --label switched path. A sequence of hops (Router 0...Router n). A packet travels from R0 to Rn by means of label switching mechanisms. An LSP can be chosen dynamically, based on normal routing mechanisms, or it can be configured manually.

**LSR** --label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MPLS** --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along the normal routing paths (sometimes called MPLS hop-by-hop forwarding).

**prefix** --The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are the network bits. For example, 1.0.0.0/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 10.0.

**RIB** --Routing Information Base. A central repository of routes that contains Layer 3 reachability information and destination IP addresses or prefixes. The RIB is also known as the routing table.

**RP** --Route Processor. The processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a supervisory processor.

**RSP** --Route Switch Processor. The processor module used in the Cisco 7500 series routers that integrates the functions of the Route Processor (RP) and the Switch Processor (SP).

**SP** --Switch Processor. The Cisco 7000-series processor module that acts as the administrator for all CxBus activities. It is sometimes called a CiscoBus controller.

**VIP** --Versatile Interface Processor. An interface card used in Cisco 7000 and Cisco 7500 series routers. The VIP provides multilayer switching and runs Cisco IOS.

**VPN** --Virtual Private Network. A router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** --A Virtual Private Network (VPN) routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

CHAPTER 3

# Configuring Basic Cisco Express Forwarding

This module contains information about Cisco Express Forwarding and describes the required and optional tasks for verifying Cisco Express Forwarding operation.

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet, and networks characterized by intensive web-based applications or interactive sessions.

## Prerequisites for Cisco Express Forwarding

Cisco Express Forwarding requires a software image that includes Cisco Express Forwarding and IP routing enabled on the device.

## Restrictions for Cisco Express Forwarding

The Cisco ASR 1000 Series Aggregation Services Routers operate only in distributed Cisco Express Forwarding mode.

## Information About Cisco Express Forwarding

If your network architecture requires that you disable or reenable Cisco Express Forwarding or distributed Cisco Express Forwarding switching and forwarding, change your load balancing scheme, refresh Cisco Express Forwarding tables, configure network accounting for Cisco Express Forwarding, or customize the display of Cisco Express Forwarding events, go to the "Related Documents" section for links to information on these tasks. Otherwise, you need do nothing more to configure Cisco Express Forwarding or distributed Cisco Express Forwarding operation in your network.

**Note** Cisco Express Forwarding is supported on interfaces on which IEEE 802.1Q encapsulation has been enabled at the subinterface level. You no longer need to disable Cisco Express Forwarding operation on interfaces that are using IEEE 802.1Q encapsulation on VLAN subinterfaces.

# Cisco Platform Support for CEF and dCEF

Cisco Express Forwarding is enable by default on the Cisco ASR 1000 Series Aggregation Services Routers.

To find out if Cisco Express Forwarding is enabled by default on your platform, enter the **show ip cef**command. If Cisco Express Forwarding is enabled, you receive output that looks like the following:

```
Router# show ip cef
Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet2/1/0
[...]
```

If Cisco Express Forwarding is not enabled on your platform, the output for the **show ip cef**command looks like this:

```
Router# show ip cef
%CEF not running
```

If Cisco Express Forwarding is not enabled on your platform, use the **ip cef**command to enable Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

# Cisco Express Forwarding Benefits

- Improved performance--Cisco Express Forwarding is less CPU-intensive than fast switching route caching. As a result, more CPU processing power can be dedicated to Layer 3 services such as quality of service (QoS) and encryption.
- Scalability--Cisco Express Forwarding offers full switching capacity at each line card when distributed Cisco Express Forwarding mode is active. Distributed Cisco Express Forwarding is a distributed switching mechanism that scales linearly with the number of interface cards and the bandwidth installed in the router.
- Resiliency--Cisco Express Forwarding offers an unprecedented level of switching consistency and stability in large dynamic networks. In dynamic networks, fast-switched cache entries are frequently invalidated by routing changes. These changes can cause traffic to be process-switched through use of the routing table, rather than fast-switched through use of the route cache. Because the forwarding information base (FIB) lookup table contains all known routes that exist in the routing table, it eliminates the need for route cache maintenance and the steps involved with fast-switch or process-switch forwarding. Cisco Express Forwarding can switch traffic more efficiently than typical demand caching schemes.

## Main Components for CEF Operation

Information conventionally stored in a route cache is stored in several data structures for Cisco Express Forwarding switching. The data structures provide optimized lookup for efficient packet forwarding. The two main components of Cisco Express Forwarding operation are the forwarding information base (FIB) and the adjacency tables.

The FIB is conceptually similar to a routing table or information base. A router uses this lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The FIB is updated as changes occur in the network and contains all routes known at the time. For more information on the FIB, see the "Cisco Express Forwarding Overview" module.

Adjacency tables maintain Layer 2 next-hop addresses for all FIB entries. For more information on adjacency tables, see the "Cisco Express Forwarding Overview" module.

This separation of the reachability information (in the Cisco Express Forwarding table) and the forwarding information (in the adjacency table), provides two main benefits:

- The adjacency table can be built separately from the Cisco Express Forwarding table, allowing both tables to build without the process switching of any packets.
- The MAC header rewrite used to forward a packet isn't stored in cache entries, so changes in a MAC header rewrite string do not require invalidation of cache entries.

# How to Verify Basic Cisco Express Forwarding

There are no configuration tasks. Cisco Express Forwarding is enabled by default.

The following section contains instructions for verifying basic Cisco Express Forwarding or distributed Cisco Express Forwarding operation.

Before you perform the remaining tasks in this section you need to know which mode of Cisco Express Forwarding is running on your router. Distributed Cisco Express Forwarding is enabled by default on the Cisco ASR 1000 Series Routers. To determine if Cisco Express Forwarding or distributed Cisco Express Forwarding is enabled on your router, you can enter the **show ip interface** command and look for the entry "IP CEF switching enabled" or "IP Distributed CEF switching enabled." If Cisco Express Forwarding is not enabled, the entry in the command display would indicate that "IP CEF switching is disabled."

To verify basic Cisco Express Forwarding or distributed Cisco Express Forwarding operation, perform the following procedures and tasks:

## Determining How the Router Is Configured

To determine if the router is configured for Cisco Express Forwarding or distributed Cisco Express Forwarding, perform the following task.

### SUMMARY STEPS

1. **enable**
2. **show ip interface** [*type slot* / *subslot* / *port*[**.** *subinterface-number*]] [**brief**]
3. **disable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show ip interface** [*type slot* / *subslot* / *port*[**.** *subinterface-number*]] [**brief**]<br>**Example:**<br>`Router# show ip interface` | Configures an interface type and enters interface configuration mode.<br>• The *type* argument is the type of interface to be configured.<br>• The *slot* argument is the chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.<br>• The / *subslot* keyword and argument pair is the secondary slot number on a SIP where a SPA is installed. The slash (/) is required.<br>Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.<br>• The / *port* keyword and argument pair is the port or interface number. The slash (/) is required.<br>Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide.<br>• The **.** *subinterface-number*keyword and argument pair is the subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs.<br>• The **brief** keyword displays a summary of the usability status information.<br>Look for the entry "IP CEF switching enabled" or "IP Distributed CEF switching enabled." |
| **Step 3** | **disable**<br>**Example:** | Exits to user EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# disable` | |

## What to Do Next

# Verifying Cisco Express Forwarding Operation

Perform the following tasks, in the order presented, to verify Cisco Express Forwarding operation on your router or to look for Cisco Express Forwarding operation information on your router:

See the Verifying Distributed Cisco Express Forwarding Operation, on page 26 for the tasks to perform for distributed Cisco Express Forwarding operation.

## Verifying That Cisco Express Forwarding Switching Is Enabled

To verify that Cisco Express Forwarding switching is enabled on the input (ingress) interface on the router, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show ip cef**
3. **show cef interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
4. **show ip interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
5. **disable**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip cef**

Use this command to verify that Cisco Express Forwarding is enabled globally. For example:

**Example:**

```
Router# show ip cef
%CEF not running
```

If Cisco Express Forwarding is not running, use the **ip cef**command to enable Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

When Cisco Express Forwarding or distributed Cisco Express Forwarding is enabled, the **show ip cef**command shows a brief display of all FIB entries.

**Step 3** **show cef interface** *type* *slot* / *subslot* / *port* [**.** *subinterface-number*]

Use this command to verify that Cisco Express Forwarding is enabled on a particular ingress interface. Look for the entry "IP CEF switching enabled." For example:

**Example:**

```
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 ! <==== Notice this entry
.
  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
```

**Step 4** **show ip interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]

Use this command to display the Cisco IOS switching methods enabled on an interface. For example:

**Example:**

```
Router# show ip interface fastethernet 1/0/0

 FastEthernet1/0/0 is up, line protocol is up

   IP fast switching is enabled
   IP fast switching on the same interface is enabled
   IP Flow switching is disabled
   IP CEF switching is enabled ! <--- Entry verifying Cisco Express Forwarding is enabled.
   IP Distributed switching is enabled
   IP Fast switching turbo vector
   IP Normal CEF switching turbo vector
   IP multicast fast switching is enabled
   IP multicast distributed fast switching is disabled
   IP route-cache flags are Fast, Distributed, No CEF         ! <--- HERE.
```

In the above output, the "IP CEF switching is enabled" entry indicates that Cisco Express Forwarding is enabled by default. The "No CEF" IP route-cache flag indicates that Cisco Express Forwarding is disabled because an administrator entered the **no ip route-cache cef**command on this interface.

To enable Cisco Express Forwarding on this interface, enter the **ip route-cache cef** command. Once you do that, the "CEF" flag indicates that Cisco Express Forwarding is running.

**Step 5** **disable**

Use this command to exit privileged EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

## Locating the Prefix in a Forwarding Table on the RP

To locate the prefix in a forwarding table, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show ip cef**
3. **show ip cef vrf** *vrf-name*
4. Repeat Step 2 as many times as required to locate the prefix.
5. **disable**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip cef**

Use this command to show entries in the FIB and confirm that prefixes are listed in the FIB. For example:

**Example:**

```
Router# show ip cef
Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet2/1/0
[...]
```

**Step 3** **show ip cef vrf** *vrf-name*

Use this command to locate prefixes in forwarding tables associated with Virtual Private Network (VPN) routing/forwarding table instances (VRFs). For example, this command shows prefixes in the left-hand column for a VRF named vpn1:

**Example:**

```
Router# show ip cef vrf vpn1
Prefix              Next Hop            Interface
0.0.0.0/32          receive
10.1.0.0/8          10.0.0.1            FastEthernet1/0/3
10.2.0.0/8          10.0.0.2            POS2/0/0
10.0.0.0/8          attached            FastEthernet1/0/3
10.0.0.0/32         receive
10.0.0.1/32         10.0.0.1            FastEthernet1/0/3
10.0.0.2/32         receive
10.255.255.255/32   receive
10.3.0.0/8          10.0.0.2            POS2/0/0
10.50.0.0/24        receive
255.255.255.255/32  receive
```

**Step 4** Repeat Step 2 as many times as required to locate the prefix.

If Cisco Express Forwarding is in a VPN, you might need to look at multiple VRFs.

**Step 5** **disable**

Use this command to exit privileged EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

## Finding the Cisco Express Forwarding Output Information

To find the Cisco Express Forwarding output information associated with the prefix on the RP, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show ip cef**
3. **show ip cef** *prefix*
4. **show ip cef** *prefix* **detail**
5. **disable**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip cef**

Use this command to confirm that the prefix is listed in the FIB. For example:

**Example:**

```
Router# show ip cef
Prefix              Next Hop            Interface
0.0.0.0/32          receive
192.168.0.0/30      attached            Serial2/0/0:1
192.168.0.0/32      receive
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
```

**Step 3** **show ip cef** *prefix*

Use this command to display the prefix entry in the FIB for centralized Cisco Express Forwarding. For example:

**Example:**

```
Router# show ip cef 10.2.61.8 255.255.255.0
10.0.0.0/8, version 72, per-destination sharing
0 packets, 0 bytes
  via 192.168.100.1, 0 dependencies, recursive
    traffic share 1
    next hop 192.168.100.1, FastEthernet1/0/0 via 192.168.100.1/32
    valid adjacency
  via 192.168.101.1, 0 dependencies, recursive
    traffic share 1
    next hop 192.168.101.1, FastEthernet2/1/0 via 192.168.101.1/32
    valid adjacency
  0 packets, 0 bytes switched through the prefix
```

**Step 4** **show ip cef** *prefix* **detail**

Use this command to show more detail for each of the active paths associated with a destination prefix. For example:

**Example:**

```
Router# show ip cef 10.0.0.0 detail
10.0.0.0/8, version 72, per-destination sharing
0 packets, 0 bytes
  via 192.168.100.1, 0 dependencies, recursive
    traffic share 1
    next hop 192.168.100.1, FastEthernet1/0/0 via 192.168.100.1/32
    valid adjacency
  via 192.168.101.1, 0 dependencies, recursive
    traffic share 1
    next hop 192.168.101.1, FastEthernet2/1/0 via 192.168.101.1/32
    valid adjacency
  0 packets, 0 bytes switched through the prefix
```

**Step 5** **disable**

Use this command to exit privileged EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

## Verifying the Adjacency or Next-Hop Information

To verify the adjacency or next-hop information, perform the following steps.

Adjacencies are added to the adjacency table when the adjacency is

- Indirectly configured manually
- Dynamically discovered through ARP
- Created when a routing protocol, for example, Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF), forms a neighbor relationship

For more information on adjacencies, see the "Cisco Express Forwarding Overview" module.

### SUMMARY STEPS

1. **enable**
2. **show ip cef**
3. **show adjacency detail**
4. **show adjacency summary**
5. **show adjacency** *type slot* **/** *subslot* **/** *port* [**.** *subinterface-number*]
6. **show ip cef exact-route** *source-address destination-address*
7. **disable**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip cef**

Use this command to find the output interface. For example:

**Example:**

```
Router# show ip cef
Prefix              Next Hop            Interface
0.0.0.0/32          receive
192.168.0.0/30      attached            Serial2/0/0:1
192.168.0.0/32      receive
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
```

In this example, the output interface for the prefix 10.2.61.8/24 is FastEthernet 1/0/0, and the next hop address is 192.168.100.1.

**Step 3** **show adjacency detail**

Use this command to display adjacency information, including Layer 2 information. For example:

**Example:**

```
Router# show adjacency detail
Protocol Interface                 Address
IP       FastEthernet1/0/0         10.2.61.8(7)
                                   0 packets, 0 bytes
                                   00107BC30D5C
                                   00500B32D8200800
                                   ARP        02:01:49
```

The encapsulation string 00107BC30D5C00500B32D8200800 is that of an adjacency used for traffic switched out of a router on a FastEthernet link by means of Ethernet II encapsulation.

**Step 4** **show adjacency summary**

Use this command to display Cisco Express Forwarding adjacency table summary information. For example:

**Example:**

```
Router# show adjacency summary
Adjacency Table has 1 adjacency
  Interface                Adjacency Count
  FastEthernet1/0/0        1
```

**Step 5** **show adjacency** *type slot* **/** *subslot* **/** *port* [**.** *subinterface-number*]

Use this command to display adjacency information for a particular interface. For example:

**Example:**

```
Router# show adjacency fastethernet 2/0/3
Protocol  Interface                    Address
IP        FastEthernet2/0/3            172.20.52.1(3045)
IP        FastEthernet2/0/3            172.20.52.22(11)
```

**Step 6** **show ip cef exact-route** *source-address destination-address*

Use this command to display the exact route for a source-destination IP address pair and verify the next-hop address. For example:

**Example:**

```
Router# show ip cef exact-route 10.1.1.1 10.2.61.8
10.1.1.1         -> 10.2.61.8 :FastEthernet1/0/0 (next hop 192.168.100.1)
```

In this example, the exact route from source address 10.1.1.1 to destination address 10.2.61.8 is through interface FastEthernet1/0/0 to next hop address 192.168.100.1.

**Step 7** **disable**

Use this command to exit privileged EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

# Verifying Distributed Cisco Express Forwarding Operation

Perform the following tasks, in the order presented, to verify distributed Cisco Express Forwarding operation on your router:

## Verifying That dCEF Switching Is Enabled

To verify that distributed Cisco Express Forwarding switching is enabled on the input (ingress) interface on the line card, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show ip cef**
3. **show ip cef** *prefix type slot* **/** *subslot* **/** *port[* **.** *subinterface-number]*
4. **disable**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip cef**

Use this command to verify that Cisco Express Forwarding is enabled globally. For example:

**Example:**

```
Router# show ip cef
%CEF not running
```

If Cisco Express Forwarding is not running, use the **ip cef**command to enable (central) Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

When Cisco Express Forwarding or distributed Cisco Express Forwarding is enabled, the **show ip cef**command shows a brief display of all FIB entries.

**Step 3** **show ip cef** *prefix type slot* **/** *subslot* **/** *port[* **.** *subinterface-number]*

Use this command to verify information about interfaces on a line card. For example:

**Example:**

```
Router# show ip cef 192.68.0.0 255.255.255.0 fastethernet0/0/0
show ip cef 192.68.0.0 255.255.255.0 from slot 0:
192.68.0.0/24, version 19, epoch 0, attached, connected
0 packets, 0 bytes
  via FastEthernet0/0/0, 0 dependencies
    valid glean adjacency
```

**Step 4** **disable**

Use this command to exit privileged EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

# Interpreting Cisco Express Forwarding Command Output

Perform the following tasks to interpret information in Cisco Express Forwarding command output:

## Verifying That CEF Information Looks As Expected

Perform the following tasks to verify that the Cisco Express Forwarding information looks as you expected.

### SUMMARY STEPS

1. **enable**
2. **show ip route**
3. **show ip cef**
4. Compare the command output in Steps 2 and 3.
5. (For distributed Cisco Express Forwarding operation only) **show ip cef** *type slot* **/** *subslot* **/** *port*[**.** *subinterface-number*
6. (For distributed Cisco Express Forwarding operation only) Compare the command output in Steps 2 and 4.
7. **disable**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip route**

Use this command to look at the forwarding information contained in the IP routing table. For example:

**Example:**

```
Router# show ip route
...
     10.1.0.0/32 is subnetted, 1 subnets
O       10.1.2.3 [110/3] via 10.5.5.5, 00:00:03, POS2/0/0
```

```
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.5.5.5/32 is directly connected, POS2/0/0
C       10.5.5.0/24 is directly connected, POS2/0/0
     10.7.0.0/24 is subnetted, 1 subnets
O       10.7.8.0 [110/3] via 10.5.5.5, 00:00:04, POS2/0/0
     10.0.0.0/24 is subnetted, 2 subnets
O       10.23.64.0 [110/12] via 10.5.5.5, 00:00:04, POS2/0/0
O       10.23.66.0 [110/12] via 10.5.5.5, 00:00:04, POS2/0/0
     10.47.0.0/32 is subnetted, 1 subnets
O       10.47.0.10 [110/3] via 10.5.5.5, 00:00:04, POS2/0/0
O    172.16.57.0/24 [110/3] via 10.5.5.5, 00:00:04, POS2/0/0
     10.150.0.0/24 is subnetted, 1 subnets
C       10.150.3.0 is directly connected, POS0/0/0
O    192.168.92.0/24 [110/2] via 10.5.5.5, 00:00:04, POS2/0/0 ! <---- Compare with entry !in show ip
 cef
 command that follows.
```

In the example, c indicates a directly connected route and o represents a route discovered by means of OSPF.

**Step 3** **show ip cef**

Use this command to display entries in the FIB. For example:

**Example:**

```
Router# show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           10.5.5.5             POS2/0/0 (default route)
0.0.0.0/32          receive
10.1.2.3/32         10.5.5.5             POS2/0/0 (two paths)
                    10.150.3.9           POS0/0/0
10.5.5.0/24         attached             POS2/0/0
10.5.5.0/32         receive
10.5.5.5/32         attached             POS2/0/0 (glean adjacency)
10.5.5.6/32         receive    (our interface)
10.5.5.255/32       receive    (broadcast)
10.7.8.0/24         10.5.5.5             POS2/0/0
                    10.150.3.9           POS0/0/0
10.23.64.0/24       10.150.3.9           POS0/0/0
10.23.66.0/24       10.150.3.9           POS0/0/0 (normal route)
10.47.0.10/32       10.150.3.9           POS0/0/0
10.150.3.0/24       attached             POS0/0/0
10.150.3.0/32       receive
10.150.3.1/32       receive
10.150.3.255/32     receive
192.168.92.0/24     10.5.5.5             POS2/0/0 ! <--- Compare with entry in show
 ip
!route
command.
                    10.150.3.9           POS0/0/0
172.16.57.0/24      10.5.5.5             POS2/0/0
                    10.150.3.9           POS0/0/0
239.224.0.0/4       receive    (multicast)
255.255.255.255/32  receive    (all 1s broadcast)
```

**Step 4** Compare the command output in Steps 2 and 3.

Cisco Express Forwarding maintains the information contained in the IP routing table structured in a way that optimizes forwarding. Check that there is a one-to-one correlation between FIB entries and routing table entries. For example, the following lines from the sample output in Step 2 and Step 2 show a one-to-one correlation. The destination prefix 192.92.92.0/24, the next hop IP address 10.5.5.5, and the next-hop interface POS2/0/0 are the same.

- From the **show ip route** command output in Step 2:

**Example:**

```
O    192.168.92.0/24 [110/2] via 10.5.5.5, 00:00:04, POS2/0/0
```

- From the **show ip cef** command output in Step 3:

**Example:**

```
192.168.92.0/24      10.5.5.5             POS2/0/0
```

If there is not a one-to-one correlation, you can recreate the central FIB table by clearing the IP routing table and allowing the routing table to be rebuilt, which in turn causes the central FIB table to be repopulated with up-to-date routing information.

**Step 5** (For distributed Cisco Express Forwarding operation only) **show ip cef** *type slot* **/** *subslot* **/** *port*[**.** *subinterface-number*

Use this command to display FIB entries on all line cards. For example:

**Example:**

```
Router# show ip cef pos2/0/0
show ip cef from slot 2:
Prefix              Next Hop            Interface
0.0.0.0/0           10.5.5.5             POS2/0/0
0.0.0.0/32          receive
10.1.2.3/32         10.5.5.5             POS2/0/0
                    10.150.3.9           POS0/0/0
105.5.5.0/24        attached             POS2/0/0
10.5.5.0/32         receive
10.5.5.5/32         attached             POS2/0/0
10.5.5.6/32         receive
10.5.5.255/32       receive
10.7.8.0/24         10.5.5.5             POS2/0/0
                    10.150.3.9           POS0/0/0
10.7.54.0/24        attached             POS0/1/0
10,7.54.0/32        receive
10.7.54.3/32        receive
10.7.54.255/32      receive
10.23.64.0/24       10.150.3.9           POS0/0/0
10.23.66.0/24       10.150.3.9           POS0/0/0
10.47.0.10/32       10.150.3.9           POS0/0/0
10.150.3.0/24       attached             POS0/0/0
10.150.3.0/32       receive
10.150.3.1/32       receive
10.150.3.255/32     receive
192.168.92.0/24     10.5.5.5             POS2/0/0
                    10.150.3.9           POS0/0/0
172.16.57.0/24      10.5.5.5             POS2/0/0
                    10.150.3.9           POS0/0/0
239.224.0.0/4       receive
255.255.255.255/32  receive
```

**Step 6** (For distributed Cisco Express Forwarding operation only) Compare the command output in Steps 2 and 4.

The output from the **show ip cef**command in Step 3 should be identical to the output from the **show ip cef**command in Step 5. If the outputs are not identical, see the " Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards " module for information on synchronizing FIB entries on the RP and the line card.

**Step 7** **disable**

Use this command to exit privileged EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

## Interpreting MPLS Information in CEF Output

Perform the following steps to interpret Multiprotocol Label Switching (MPLS) information in Cisco Express Forwarding output.

Cisco Express Forwarding interacts with a label switched path (LSP) primarily at the beginning and end of the LSP--that is, on label imposition (IP packet to MPLS packet) and label disposition (MPLS packet to IP packet). Output from Cisco Express Forwarding commands should show these processes.

The Cisco implementation of MPLS leverages the advantages of Cisco Express Forwarding. When you use a router as an MPLS edge router, Cisco Express Forwarding identifies the route for incoming packets and finds the label to apply to the packet.

However, when you use a router as a label switch router (LSR), tables from the MPLS label forwarding information base (LFIB) are used to switch MPLS packets. These tables are distributed to the line cards in the same way that the FIB tables are distributed in Cisco Express Forwarding.

A customer-site VRF contains all the routes available to the site from the VPNs to which it belongs. VPN routing information is stored in the IP routing table and in the Cisco Express Forwarding table for each VRF. A separate set of tables is maintained for each VRF, which prevents information from being forwarded outside a VPN and prevents packets that are outside a VPN from being forwarded to a router within the VPN. Based on the routing information stored in the VRF IP routing table and the VRF Cisco Express Forwarding table, packets are forwarded to their destinations. Output from Cisco Express Forwarding commands shows details from the VRF Cisco Express Forwarding tables.

### SUMMARY STEPS

1. **enable**
2. **show ip cef vrf** *vrf-name* **detail**
3. **disable**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. You can also enter this command in user EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip cef vrf** *vrf-name* **detail**

Use this command to display detailed information from the Cisco Express Forwarding forwarding table that is associated with a VRF. For example:

**Example:**

```
Router# show ip cef vrf vpn1 detail

IP CEF with switching (Table Version 10), flags=0x0
  8 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
  46 leaves, 51 nodes, 54640 bytes, 361 inserts, 315 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id F968AD29
  5 CEF resets, 38 revisions of existing leaves
  refcounts:  1400 leaf, 1392 node
Adjacency Table has 2 adjacencies
0.0.0.0/32, version 0, receive
192.168.6.0/24, version 9, cached adjacency to Serial0/1.1
0 packets, 0 bytes
```

The following section of the Cisco Express Forwarding output provides MPLS information for the first adjacency. The "tag rewrite" is an equivalent of a Cisco Express Forwarding adjacency. Look at the tags imposed field. The first tag {20} is the tag used to reach the next hop, 10.1.1.13. The second tag {30} is the tag advertised to the local provider edge (PE) router by the remote PE router.

**Example:**

```
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Se0/1.1, point2point, tags imposed: {20 30}
  via 10.10.10.6, 0 dependencies, recursive
    next hop 10.1.1.13, Serial0/1.1 via 10.10.10.6
    valid cached adjacency
    tag rewrite with Se0/1.1, point2point, tags imposed: {20 30}
```

The following section of the output provides information about the second adjacency. For the second adjacency, no tag rewrite occurs as indicated by the entry "tag rewrite with , ," and MPLS tags are not imposed on the packet indicated by the entry "tags imposed : {}." The router also discards this packet indicated by the entry "valid discard adjacency."

**Example:**

```
192.168.4.0/24, version 6, attached, connected
0 packets, 0 bytes
  tag information set
    local tag: 28
  via Loopback102, 0 dependencies
    valid discard adjacency
    tag rewrite with , , tags imposed: {}
192.168.4.0/32, version 4, receive
192.168.4.1/32, version 3, receive
192.168.4.255/32, version 5, receive
192.168.0.0/24, version 2, receive
255.255.255.255/32, version 1, receive
```

**Step 3** **disable**

Use this command to exit to user EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

# Configuration Examples for Basic CEF

There are no configuration examples for Cisco Express Forwarding. Cisco Express Forwarding is enabled by default.

# Where to Go Next

If you want to disable Cisco Express Forwarding or distributed Cisco Express Forwarding operation, refer to Enabling or Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding to Customize Switching/Forwarding for Dynamic Networks.

# Glossary

**adjacency** --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

**Cisco Express Forwarding** --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor (RP) to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

**distributed Cisco Express Forwarding** --A type of Cisco Express Forwarding switching in which line cards maintain identical copies of the Forwarding Information Base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Processor of involvement in the switching operation.

**FIB** --forwarding information base. A component of Cisco Express Forwarding. The router uses the FIB lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

**IPC** --interprocess communication. The mechanism that enables the distribution of Cisco Express Forwarding tables from the Route Processor (RP) to the line card when the router is operating in distributed Cisco Express Forwarding mode.

**label disposition** --The removal of Multiprotocol Label Switching (MPLS) headers at the edge of a network. In MPLS label disposition, packets arrive on a router as MPLS packets and, with the headers removed, are transmitted as IP packets.

**label imposition** --The action of putting a label on a packet.

**LER** --label edge router. A router that performs label imposition.

**LFIB** --label forwarding information base. The data structure used by switching functions to switch labeled packets.

**LIB** --label information base. A database used by a label switch router (LSR) to store labels learned from other LSRs, as well as labels assigned by the local LSR.

**line card** --A general term for an interface processor that can be used in various Cisco products.

**LSP** --label switched path. A sequence of hops (Router 0...Router n). A packet travels from R0 to Rn by means of label switching mechanisms. An LSP can be chosen dynamically, based on normal routing mechanisms, or it can be configured manually.

**LSR** --label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MPLS** --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along the normal routing paths (sometimes called MPLS hop-by-hop forwarding).

**prefix** --The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are the network bits. For example, 1.0.0.0/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 10.0.

**RIB** --Routing Information Base. A central repository of routes that contains Layer 3 reachability information and destination IP addresses or prefixes. The RIB is also known as the routing table.

**RP** --Route Processor. The processor module contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a supervisory processor.

**VPN** --Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** --A Virtual Private Network (VPN) routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

CHAPTER 4

# Enabling or Disabling CEF or dCEF

This module contains information about Cisco Express Forwarding and describes the required and optional tasks for enabling or disabling Cisco Express Forwarding and distributed Cisco Express Forwarding. Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

## Prerequisites for Enabling or Disabling CEF or dCEF

Cisco Express Forwarding requires a software image that includes Cisco Express Forwarding and IP routing enabled on the switch or router.

# Restrictions for Enabling or Disabling CEF or dCEF

- The Cisco ASR 1000 Series Aggregation Services Router operates only in distributed Cisco Express Forwarding mode.
- 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 process switched. Logging disables Cisco Express Forwarding.

# Information About Enabling or Disabling CEF or dCEF

## Cisco Platform Support for Central CEF and dCEF

Cisco Express Forwarding is enable by default on the Cisco ASR 1000 Series Aggregation Services Routers.

To find out if Cisco Express Forwarding is enabled on your platform, enter the **show ip cef**command. If Cisco Express Forwarding is enabled, you receive output that looks like this:

```
Router# show ip cef
Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet2/1/0
[...]
```

If Cisco Express Forwarding is not enabled on your platform, the output for the **show ip cef**command looks like this:

```
Router# show ip cef
%CEF not running
```

If Cisco Express Forwarding is not enabled on your platform, use the **ip cef**command to enable central Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

## When to Enable or Disable Central CEF on a Router

Enable central Cisco Express Forwarding operation when line cards are not available for Cisco Express Forwarding switching or when you need to use features not compatible with distributed Cisco Express Forwarding switching. When central Cisco Express Forwarding operation is enabled, the Cisco Express Forwarding Forwarding Information Base (FIB) and adjacency tables reside on the RP, and the RP performs express forwarding.

Disable central Cisco Express Forwarding on a router when you want to turn off central Cisco Express Forwarding on the router and on all interfaces on the router. You might want to do this if your router and router interfaces are configured with a feature that central Cisco Express Forwarding or distributed Cisco Express Forwarding does not support.

To disable central Cisco Express Forwarding on a router and on all interfaces on the router, use the **no ip cef** command.

# When to Enable dCEF on a Line Card

Enable distributed Cisco Express Forwarding on a line card when you want the line card to perform express forwarding so that the RP can handle routing protocols or switch packets from legacy interface processors. When distributed Cisco Express Forwarding is enabled, line cards maintain an identical copy of the FIB and adjacency tables. The line cards perform express forwarding between port adapters, thus relieving the RP of involvement in the switching operation. distributed Cisco Express Forwarding uses an interprocess communication (IPC) mechanism to ensure synchronization of FIB tables and adjacency tables on the RP and line cards.

The Cisco ASR 1000 Series Routers operate only in distributed Cisco Express Forwarding mode. In other routers you can mix various types of line cards in the same router, and all of the line cards you are using need not support Cisco Express Forwarding. When a line card that does not support Cisco Express Forwarding receives a packet, the line card forwards the packet to the next higher switching layer (the RP) or forwards the packet to the next hop for processing. This structure allows legacy interface processors to exist in the router with newer interface processors.

**Note** When you enable distributed Cisco Express Forwarding globally, all interfaces that support distributed Cisco Express Forwarding are enabled by default.

# When to Enable or Disable CEF on an Interface

You need to decide whether or not you want Cisco Express Forwarding operation on an interface. 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 operation globally, you must use the **no** form of the **ip route-cache cef**command to turn off Cisco Express Forwarding operation on a particular interface. To reenable Cisco Express Forwarding, use the **ip route-cache cef** command. To reenable distributed Cisco Express Forwarding, use the **ip route-cache distributed** command.

Disabling Cisco Express Forwarding or distributed Cisco Express Forwarding on an interface disables Cisco Express Forwarding switching for packets forwarded to the interface, but has no effect on packets forwarded out of the interface.

When you disable Cisco Express Forwarding or distributed Cisco Express Forwarding, Cisco IOS XE software switches packets received on the interface using the next fastest switching path. For Cisco Express Forwarding, the next fastest switching path is switching on the RP. For distributed Cisco Express Forwarding, the next fastest switching path is Cisco Express Forwarding on the RP.

The input interface determines the Cisco IOS XE switching path that a packet takes. Consider the following when enabling or disabling switching methods on a particular interface:

- You need Cisco Express Forwarding to be enabled on the incoming interface for packets to be Cisco Express Forwarding switched.
- Because Cisco Express Forwarding makes the forwarding decision on input, you need to use the **no ip route-cache cef**command on the ingress interface if you want to disable Cisco Express Forwarding.

# How to Enable or Disable Central CEF or dCEF

To enable or disable Cisco Express Forwarding or distributed Cisco Express Forwarding, perform either of the following tasks depending on whether you want to enable or disable Cisco Express Forwarding or distributed Cisco Express Forwarding on the router or to enable or disable Cisco Express Forwarding or distributed Cisco Express Forwarding on an interface:

## Enabling or Disabling CEF or dCEF on a Router

Perform the following task to enable or disable Cisco Express Forwarding or distributed Cisco Express Forwarding operation on a router. Cisco Express Forwarding can optimize your network performance and scalability.

### SUMMARY STEPS

1. **enable**
2. **show ip cef** [**vrf** *vrf-name*] [*interface-type interface-number* [**checksum** | [**detail** | **internal** [**checksum**] | **platform**]]
3. **configure terminal**
4. **ip cef distributed**
5. **exit**
6. **show ip cef** [**vrf** *vrf-name*] [*interface-type interface-number* [**checksum** | [**detail** | **internal** [**checksum**] | **platform**]]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show ip cef** [**vrf** *vrf-name*] [*interface-type interface-number* [**checksum** \| [**detail** \| **internal** [**checksum**] \| **platform**]]<br>**Example:**<br>`Router# show ip cef` | Displays entries in the forwarding information base (FIB).<br>Use this command to determine if Cisco Express Forwarding is enabled globally and on a particular interface. If Cisco Express Forwarding is not enabled, the output displays:<br>`%CEF not running` |
| **Step 3** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ip cef distributed**<br>**Example:**<br>`Router(config)# ip cef distributed` | Enables distributed Cisco Express Forwarding operation. Cisco Express Forwarding information is distributed to line cards. Line cards perform express forwarding. |
| **Step 5** | **exit**<br>**Example:**<br>`Router(config)# end` | Exits to privileged EXEC mode. |
| **Step 6** | **show ip cef** [**vrf** *vrf-name*] [*interface-type interface-number* [**checksum** \| [**detail** \| **internal** [**checksum**] \| **platform**]]<br>**Example:**<br>`Router# show ip cef` | Displays entries in the FIB.<br>Use this command to verify that Cisco Express Forwarding is enabled. If Cisco Express Forwarding is enabled, the output displays destination prefixes, next-hop IP addresses, and next-hop interfaces. |

# Enabling or Disabling CEF or dCEF on an Interface

Perform the following task to enable or disable Cisco Express Forwarding or distributed Cisco Express Forwarding operation on an interface. Cisco Express Forwarding can optimize your network performance and scalability.

### SUMMARY STEPS

1. **enable**
2. **show cef interface** [*type slot* / *subslot* / *port*[**.** *subinterface-number*]] [**statistics**] [**detail**]
3. **configure terminal**
4. **interface** type *slot* / *subslot* / *port*[**.** *subinterface-number*]
5. **no ip route-cache cef**
6. **end**
7. **show cef interface** [*type slot* / *subslot* / *port*[**.** *subinterface-number*]] [**statistics**] [**detail**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show cef interface** [*type slot* / *subslot* / *port*[**.** *subinterface-number*]] [**statistics**] [**detail**]<br>**Example:**<br>`Router# show cef interface fastethernet 1/0/0` | Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces.<br>Look for "IP CEF switching enabled" or "IP Distributed CEF switching enabled" in the output. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 4** | **interface** type *slot* **/** *subslot* **/** *port*[**.** *subinterface-number*]<br>**Example:**<br>`Router(config)# interface fastethernet 1/0/0` | Configures an interface type and enters interface configuration mode.<br>• The *type* argument is the type of interface to be configured.<br>• The *slot* argument is the chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.<br>• The **/** *subslot* keyword and argument pair is the secondary slot number on a SIP where a SPA is installed. The slash (/) is required.<br>Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.<br>• The **/** *port* keyword and argument pair is the port or interface number. The slash (/) is required.<br>Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide<br>• The **.** *subinterface-number*keyword and argument pair is the subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs. |
| **Step 5** | **no ip route-cache cef**<br>**Example:**<br>`Router(config-if)# no ip route-cache cef` | Disables Cisco Express Forwarding operation on an interface.<br>• The **ip cef route-cache cef** command enables distributed Cisco Express Forwarding operation on an interface after distributed Cisco Express Forwarding operation was disabled. |
| **Step 6** | **end**<br>**Example:** | Exits to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config)# end` | |
| **Step 7** | **show cef interface** [*type slot* / *subslot* / *port*[**.** *subinterface-number*]] [**statistics**] [**detail**]<br>**Example:**<br>`Router# show cef interface fastethernet 1/0/0` | Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces.<br>Verify that "IP CEF switching enabled" or "IP Distributed CEF switching enabled" is displayed in the output. |

# Configuration Examples for Central CEF or dCEF

## Example Enabling or Disabling CEF or dCEF on a Router

You might want to disable distributed Cisco Express Forwarding if your router and router interfaces are configured with a feature that distributed Cisco Express Forwarding does not support. The following example shows how to disable distributed Cisco Express Forwarding on a router:

```
configure terminal
!

no ip cef distributed

end
```

## Example Enabling or Disabling Central CEF or dCEF on an Interface

All interfaces that support Cisco Express Forwarding operation (central Cisco Express Forwarding or distributed Cisco Express Forwarding) are enabled by default when you enable Cisco Express Forwarding operation globally. You might want to disable central Cisco Express Forwarding or distributed Cisco Express Forwarding on a particular interface if that interface is configured with a feature that central Cisco Express Forwarding or distributed Cisco Express Forwarding does not support.

The following example shows how to disable central Cisco Express Forwarding on a particular interface:

```
configure terminal
!
interface ethernet 1/1/0
 no ip route-cache cef
 end
```

The following example shows how to disable distributed Cisco Express Forwarding on FastEthernet interface 0/0/0:

```
configure terminal
!
interface fe0/0/0
 no ip route-cache cef
 end
```

The following example shows how to reenable distributed Cisco Express Forwarding operation on FastEthernet interface 0/0/0:

```
configure terminal
!
ip cef distributed
!
interface fe0/0/0
# ip route-cache cef
 end
```

The following example shows how to enable distributed Cisco Express Forwarding operation on the router (globally) and turn off Cisco Express Forwarding operation on FastEthernet interface 0/0/0:

```
configure terminal
!
ip cef distributed
interface fe0/0/0
 no ip route-cache cef
 end
```

The following example shows how to reenable distributed Cisco Express Forwarding operation on FastEthernet interface 0/0/0:

```
configure terminal
!
ip cef distributed
!
interface fe0/0/0
 ip route-cache cef
 end
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Commands for configuring and managing Cisco Express Forwarding | *Cisco IOS IP Switching Command Reference* |
| Overview of the Cisco Express Forwarding feature | Cisco Express Forwarding Overview |
| Tasks for verifying Cisco Express Forwarding information on your router | Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks |
| Tasks for configuring a load-balancing scheme for Cisco Express Forwarding | Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic |
| Tasks for configuring Cisco Express Forwarding consistency checkers | Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards |

| Related Topic | Document Title |
|---|---|
| Tasks for configuring epochs for Cisco Express Forwarding tables | Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables |
| Tasks for configuring and verifying Cisco Express Forwarding network accounting | Configuring Cisco Express Forwarding Network Accounting |
| Tasks for customizing the display of Cisco Express Forwarding event trace messages | Customizing the Display of Cisco Express Forwarding Event Trace Messages |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | -- |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Enabling or Disabling CEF or dCEF

*Table 4: Feature Information for Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| This table is intentionally left blank because no features were introduced or modified in Cisco IOS XE Release 2.1or later. This table will be updated when feature information is added to this module. | -- | -- |

# Glossary

**adjacency** --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

**Cisco Express Forwarding** --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

**distributed Cisco Express Forwarding** --A mode of Cisco Express Forwarding operation in which line cards maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Processor of involvement in the switching operation.

**FIB** --forwarding information base. A component of Cisco Express Forwarding that is conceptually similar to a routing table or information base. The router uses the FIB lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

**GRE** --generic routing encapsulation. A tunneling protocol developed by Cisco that enables encapsulation of a wide variety of protocol packet types inside IP tunnels. GRE creates a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows the expansion of a network across a single-protocol backbone environment.

**IPC** --interprocess communication. The mechanism that enables the distribution of Cisco Express Forwarding tables from the Route Processor (RP) to the line card when the router is operating in distributed Cisco Express Forwarding mode.

**label disposition** --The removal of Multiprotocol Label Switching (MPLS) headers at the edge of a network. In MPLS label disposition, packets arrive on a router as MPLS packets and, with the header removed, are transmitted as IP packets.

**label imposition** --The action of putting a label on a packet.

**LER** --label edge router. A router that performs label imposition.

**LFIB** --Label Forwarding Information Base. The data structure used by switching functions to switch labeled packets.

**LIB** --Label information base. A database used by a label switch router (LSR) to store labels learned from other LSRs, as well as labels assigned by the local LSR.

**line card** --A general term for an interface processor that can be used in various Cisco products.

**LSP** --label switched path. A sequence of hops (Router 0...Router n). A packet travels from R0 to Rn by means of label switching mechanisms. An LSP can be chosen dynamically, based on normal routing mechanisms, or you can configure the LSP manually.

**LSR** --label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MPLS** --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along the normal routing paths (sometimes called MPLS hop-by-hop forwarding).

**prefix** --The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are the network bits. For example, 1.0.0.0/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 10.0.

**RIB** --Routing Information Base. A central repository of routes that contains Layer 3 reachability information and destination IP addresses or prefixes. The RIB is also known as the routing table.

**RP** --Route Processor. The processor module in the router that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a supervisory processor.

**VPN** --Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** --A Virtual Private Network (VPN) routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

CHAPTER 5

# Configuring a Load-Balancing Scheme

This module contains information about Cisco Express Forwarding and describes the tasks for configuring a load-balancing scheme for Cisco Express Forwarding traffic. Load-balancing allows you to optimize resources by distributing traffic over multiple paths.

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

## Prerequisites for a Load-Balancing Scheme

- Cisco Express Forwarding or distributed Cisco Express Forwarding must be enabled on your switch or router.
- If you enable per-packet load balancing for traffic going to a particular destination, all interfaces that can forward traffic to that destination must be enabled for per-packet load balancing.

# Restrictions for a Load-Balancing Scheme

# Information About a Load-Balancing Scheme

## Cisco Platform Support for Central CEF and dCEF

To find out if Cisco Express Forwarding is enabled on your platform, enter the **show ip cef**command. If Cisco Express Forwarding is enabled, you receive output that looks like this:

```
Router# show ip cef
Prefix             Next Hop           Interface
[...]
10.2.61.8/24       192.168.100.1      FastEthernet1/0/0
                   192.168.101.1      FastEthernet6/1
[...]
```

If Cisco Express Forwarding is not enabled on your platform, the output for the **show ip cef**command looks like this:

```
Router# show ip cef
%CEF not running
```

When distributed Cisco Express Forwarding is enabled on your platform, the line cards perform the express forwarding.

If Cisco Express Forwarding is not enabled on your platform, use the **ip cef**command to enable (central) Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

## CEF Load-Balancing Overview

Cisco Express Forwarding load balancing is based on a combination of source and destination packet information; it allows you to optimize resources by distributing traffic over multiple paths.

You can configure load balancing on a per-destination or per-packet basis. Because load-balancing decisions are made on the outbound interface, load balancing must be configured on the outbound interface.

## Per-Destination Load Balancing

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

Per-destination load balancing is enabled by default when you enable Cisco Express Forwarding. To use per-destination load balancing, you do not perform any additional tasks once Cisco Express Forwarding is enabled. Per-destination is the load-balancing method of choice for most situations.

Because per-destination load balancing depends on the statistical distribution of traffic, load sharing becomes more effective as the number of source-destination host pairs increases.

You can use per-destination load balancing to ensure that packets for a given host pair arrive in order. All packets intended for a certain host pair are routed over the same link (or links).

Typically, you disable per-destination load balancing when you want to enable per-packet load balancing.

# Per-Packet Load Balancing

Cisco Express Forwarding Per-packet load balancing allows the router to send successive data packets over different paths without regard to individual hosts or user sessions. It uses the round-robin method to determine which path each packet takes to the destination. Per-packet load balancing ensures that the traffic is balanced over multiple links.

Per-packet load balancing is good for single-path destinations, but packets for a given source-destination host pair might take different paths. Per-packet load balancing can therefore introduce reordering of packets. This type of load balancing is inappropriate for certain types of data traffic (such as voice traffic over IP) that depend on packets arriving at the destination in sequence.

Use per-packet load balancing to help ensure that a path for a single source-destination host pair does not get overloaded. If the bulk of the data passing through parallel links is for a single pair, per-destination load balancing overloads a single link while other links have very little traffic. Enabling per-packet load balancing allows you to use alternate paths to the same busy destination.

**Note** Although per-packet load balancing is intended for use on the majority of Cisco IOS routers, it is not supported on the Cisco ASR 1000 (and higher) Series Aggregation Services Router. Also, per-packet load balancing can result in out-of-sequence (OOS) packet delivery errors on some routers, which can cause applications such as VoIP to malfunction. Therefore, per-packet load balancing is not recommended. For more information, see the release notes and caveats for your platform and software release.

# Load-Balancing Algorithms

The following load-balancing algorithms are provided for use with Cisco Express Forwarding traffic. You select a load-balancing algorithm with the **ip cef load-sharing algorithm** command.

- Original algorithm--The original Cisco Express Forwarding load-balancing algorithm produces distortions in load sharing across multiple routers because the same algorithm was used on every router. Depending on your network environment, you should select either the universal algorithm (default) or the tunnel algorithm instead.
- Universal algorithm--The universal load-balancing algorithm allows each router on the network to make a different load sharing decision for each source-destination address pair, which resolves load-sharing imbalances. The router is set to perform universal load sharing by default.
- Tunnel algorithm--The tunnel algorithm is designed to balance the per-packet load when only a few source and destination pairs are involved.
- Include-ports algorithm--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.

## GTP-U TEID-Based ECMP Load-Balancing Algorithm for Cisco IOS XE Software

GPRS Tunneling Protocol (GTP) is mainly used to deliver mobile data on wireless networks via the Cisco ASR 1000 Series Aggregation Services Routers as the core router. When two routers carrying GTP traffic are connected with equal-cost multi-path (ECMP) routing between them, you can use the **show ip cef exact-route** *source - ip address* [**src-port** *port number*] *destination-ip address*[ **dest-port** *port number*] [ **gtp-teid** *teid*] command in the User EXEC mode or the Privileged EXEC mode to verify the interface selected for load balancing.

To achieve load balancing, the Cisco ASR 1000 Series Aggregation Services Routers use a 4-tuple source IP address, destination IP address, L4 source and destination port (if traffic is TCP or UDP), and fields from the packet. However, for GTP traffic, the presence of limited number of unique values for these fields restricts the equal distribution of traffic load on the tunnel. To avoid polarization for GTP traffic in load balancing, a tunnel endpoint identifier (TEID) in the GTP header is used instead of the UDP port number. Because TEID is unique per tunnel, traffic can be evenly load balanced across ECMPs. This feature allows you to look inside the GTP header and balance the traffic over ECMP on a per subscriber basis.

In Cisco IOS XE platforms, the RIB allows up to 32 paths, whereas CEF allows up to 16 paths. The CIsco IOS XE platforms can further limit the number of supported paths. When the number of paths available for forwarding to certain destinations exceeds the upper limit limit, CEF divides the set of available paths into two or more load balance objects each with an equal number of paths.

For example, if for a route there are twenty paths and the load balance limit is sixteen, CEF creats two load balance objects with ten paths in each and then also decides which of the two load balance objects to use for forwarding this route. In a hypothetical scenario where two prefixes share the same forwarding information, each may end up using a different load balance object therefore ensuring that all twenty available paths are utilised.

The GTP-U TEID-Based ECMP Load-Balancing Algorithm feature adds support for:

- GTP with IPv4 and IPv6 transport header on physical interface
- GTP traffic over the Traffic Engineering (TE) tunnel, which supports load balancing between different TE tunnels
- GTPv1-U with UDP port 2152
- Up to 8 ECMP paths

### Restrictions for GTP-U TEID-Based ECMP Load-Balancing Algorithm

The following restrictions apply to the GTP-U TEID-Based ECMP Load-Balancing Algorithm feature:

- GTPv0 is not supported to avoid extra performance impact.
- GTP-C and GTP over L2VPN are not supported.

### Enabling the GTP-U TEID Load-Balancing Algorithm

Use the **ip cef load-sharing algorithm include-ports source destination gtp** command to enable the GTP-U TEID load-balancing algorithm for IPv4.

Use the **ipv6 cef load-sharing algorithm include-ports source destination gtp** command to enable the GTP-U TEID load-balancing algorithm for IPv6.

Use the **show ip cef exact-route** *source - ip address* [**src-port** *port number*] *destination-ip address* [**dest-port** *port number*] [ **gtp-teid** *teid*] command to display the exact route of GTP-U TEID for IPv4.

Use the **show ipv6 cef exact-route** *source-ip address* [**src-port** *port number*] *destination-ip address* [**dest-port** *port number*] [**gtp-teid** *teid*] command to display the exact route of GTP-U TEID for IPv6.

# How to Configure a Load-Balancing Scheme

## Enabling or Disabling Per-Destination Load Balancing

Perform this task to enable or disable Cisco Express Forwarding per-destination load balancing.

Typically, you disable per-destination load balancing when you want to enable per-packet load balancing.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface** *type slot* / *port*
   - 
   - **interface** *type slot* / *port-adapter* / *port*
4. [**no**] **ip load-sharing per-destination**
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | Do one of the following:<br>• **interface** *type slot* / *port*<br>•<br>• **interface** *type slot* / *port-adapter* / *port*<br>**Example:**<br>`Router(config)# interface ethernet 1/1`<br>**Example:**<br>`or` | Configures an interface type and enters interface configuration mode.<br>• The *type* argument specifies the type of interface to be configured.<br>• The *slot* argument specifies the slot number. Refer to the appropriate hardware manual for slot and port information.<br>• The *port* argument specifies the port number. Refer to the appropriate hardware manual for slot and port information. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router(config)# interface fastethernet 1/0/0` | - The *port-adapter*argument specifies the port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.<br>**Note** The slashes after the *slot*argument and *port-adapter*argument are required. |
| **Step 4** | [**no**] **ip load-sharing per-destination**<br>**Example:**<br>`Router(config-if)# no ip load-sharing per-destination` | Enables per-destination load balancing for Cisco Express Forwarding on the interface.<br>**Note** The **no ip load-sharing** command disables load balancing for Cisco Express Forwarding on the interface. |
| **Step 5** | **end**<br>**Example:**<br>`Router(config-if)# end` | Exits to privileged EXEC mode. |

# Configuring Per-Packet Load Balancing

Perform the following task to configure Cisco Express Forwarding per-packet load balancing.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface** *type slot* / *port*
   -
   - **interface** *type slot* / *port-adapter* / *port*
4. **ip load-sharing per-packet**
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# configure terminal` | |
| **Step 3** | Do one of the following:<br>• **interface** *type slot* / *port*<br>•<br>• **interface** *type slot* / *port-adapter* / *port*<br>**Example:**<br>`Router(config)# interface ethernet 1/1`<br>**Example:**<br>`or`<br>**Example:**<br>`Router(config)# interface fastethernet 1/0/0` | Configures an interface type and enters interface configuration mode.<br>• The *type* argument specifies the type of interface to be configured.<br>• The *slot*argument specifies the slot number. Refer to the appropriate hardware manual for slot and port information.<br>• The *port* argument specifies the port number. Refer to the appropriate hardware manual for slot and port information.<br>• The *port-adapter*argument specifies the port adapter number. Refer to the appropriate hardware manual for information about port adapters.<br>**Note** The slashes after the *slot*argument and *port-adapter*argument are required. |
| **Step 4** | **ip load-sharing per-packet**<br>**Example:**<br>`Router(config-if)# ip load-sharing per-packet` | Enables per-packet load balancing for Cisco Express Forwarding on the interface. |
| **Step 5** | **end**<br>**Example:**<br>`Router(config-if)# end` | Exits to privileged EXEC mode. |

# Selecting a Tunnel Load-Balancing Algorithm

Perform the following task to select a tunnel load-balancing algorithm for Cisco Express Forwarding traffic. Select the tunnel algorithm when your network environment contains only a few source and destination pairs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef load-sharing algorithm** {**original** | **tunnel** [*id*] | **universal** [*id*] | **include-ports** {**source**[*id*]| [**destination**] [*id*] | **source**[*id*] **destination** [*id*]}}
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip cef load-sharing algorithm** {**original** \| **tunnel** [*id*] \| **universal** [*id*] \| **include-ports** {**source**[*id*]\| [**destination**] [*id*] \| **source**[*id*] **destination** [*id*]}}<br>**Example:**<br>`Router(config)# ip cef load-sharing algorithm tunnel` | Selects a Cisco Express Forwarding load-balancing algorithm.<br>• The **original** keyword sets the load-balancing algorithm to the original algorithm, based on a source and destination hash.<br>• The **tunnel** keyword sets the load-balancing algorithm to one that can be used in tunnel environments or in environments where there are only a few IP source and destination address pairs.<br>• The *id* argument is a fixed identifier.<br>• The **universal** keyword sets the load-balancing algorithm to one that uses a source and destination and an ID hash.<br>• The **include-ports source** keywords set the load-balancing algorithm to one that uses the source port.<br>• The **include-ports destination** keywords set the load-balancing algorithm to one that uses the destination port.<br>• The **include-ports source destination**keywords set the load-balancing algorithm to one that uses both source and destination ports. |
| **Step 4** | **end**<br>**Example:**<br>`Router(config)# end` | Exits to privileged EXEC mode. |

# Configuration Examples for a Load-Balancing Scheme

## Example Enabling or Disabling Per-Destination Load Balancing

Per-destination load balancing is enabled by default when you enable Cisco Express Forwarding. Typically, you disable per-destination load balancing when you want to enable per-packet load balancing. The following example shows how to disable per-destination load balancing:

```
configure terminal

!

interface ethernet 1/1

 no ip load-sharing per-destination
 end
```

## Example Configuring Per-Packet Load Balancing

The following example shows how to configure per-packet load balancing for Cisco Express Forwarding:

```
configure terminal
!

interface ethernet 1/1

 ip load-sharing per-packet
 end
```

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

## Example Selecting a Tunnel Load-Balancing Algorithm

The following example shows how to select a tunnel load-balancing algorithm for Cisco Express Forwarding:

```
configure terminal
!

ip cef load-sharing algorithm tunnel

end
```

The following example shows how to disable the tunnel load-balancing algorithm:

```
configure terminal
!
```

```
no ip cef load-sharing algorithm tunnel

end
```

## Example Selecting an Include-Ports Layer 4 Load-Balancing Algorithm

The following example shows how to select an include-ports Layer 4 load-balancing algorithm for Cisco Express Forwarding traffic:

```
configure terminal
!

ip cef load-sharing algorithm include-ports source

end
```

This example sets up load sharing that includes the source port in the load-balancing decision.

To disable the include-ports Layer 4 load-balancing algorithm and return to the default universal mode, enter the following commands:

```
configure terminal
!

no ip cef load-sharing algorithm

end
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples. | *Cisco IOS IP Switching Command Reference* |
| Overview of the Cisco Express Forwarding feature | Cisco Express Forwarding Overview |
| Tasks for verifying basic Cisco Express Forwarding and distributed Cisco Express Forwarding operation | Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks |
| Tasks for enabling or disabling Cisco Express Forwarding or distributed Cisco Express Forwarding | Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding to Customize Switching and Forwarding for Dynamic Network |

| Related Topic | Document Title |
|---|---|
| Tasks for configuring Cisco Express Forwarding consistency checkers | Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards |
| Tasks for configuring epochs for Cisco Express Forwarding tables | Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables |
| Tasks for configuring and verifying Cisco Express Forwarding network accounting | Configuring Cisco Express Forwarding Network Accounting |
| Tasks for customizing the display of recorded Cisco Express Forwarding events | Customizing the Display of Recorded Cisco Express Forwarding Events |
| Explanation of and troubleshooting information for the Cisco IOS software implementation of Layer 3 load balancing across multiple parallel links when Cisco Express Forwarding is used | Troubleshooting Load Balancing Over Parallel Links Using Cisco Express Forwarding |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | -- |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for a Load-Balancing Scheme

*Table 5: Feature Information for Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| GTP-U TEID-Based ECMP Load-Balancing Algorithm for Cisco IOS XE Software | Cisco IOS XE Release 3.10S | This feature allows CEF to use the GPRS Tunneling Protocol Tunnel Endpoint Identifier (GTP TEID) load-balancing algorithm. |

# Glossary

**adjacency** --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

**Cisco Express Forwarding** --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

**distributed Cisco Express Forwarding** --A mode of Cisco Express Forwarding operation in which line cards (such as Versatile Interface Processor [VIP] line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

**FIB** --forwarding information base. A component of Cisco Express Forwarding that is conceptually similar to a routing table or information base. The router uses the FIB lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

**LSP** --label switched path. A sequence of hops (Router 0...Router n). A packet travels from R0 to Rn by means of label switching mechanisms. An LSP can be chosen dynamically, based on normal routing mechanisms, or you can configure the LSP manually.

**prefix** --The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are the network bits. For example, 1.0.0.0/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 10.0.

**RIB** --Routing Information Base. A central repository of routes that contains Layer 3 reachability.

CHAPTER 6

# Load Balancing Application Flows Using Deep Packet Inspection Algorithm

The Deep Packet Inspection (DPI) algorithm helps in identification of application flows to facilitate detailed inspection of packets. The DPI algorithm deeply inspects the packets and therefore helps the service provider identify efficient ways to share bandwidth among parallel ethernet interfaces.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

## Information About Load Balancing Using Deep Packet Inspection Algorithm

### Packet Inspection and Identification Using Hash Value

The DPI algorithm performs deep inspection of packets to generate a unique hash value that helps in identification of packets that flow into parallel links. This helps in effective sharing of bandwidth among subscribers.

**Note** The packet inspection is done for both IPv4 and IPv6 traffic. If the traffic is of type PPoE, then enabling the DPI algorithm performs load balancing of the PPPoE traffic as well.

## Preserve Key Control Configuration

If you choose to remove the DPI configurations, you can do that using the command **no port-channel load-balance-hash-algo dpi algorithm** command. This will remove all the DPI tunnel and key-control configurations.

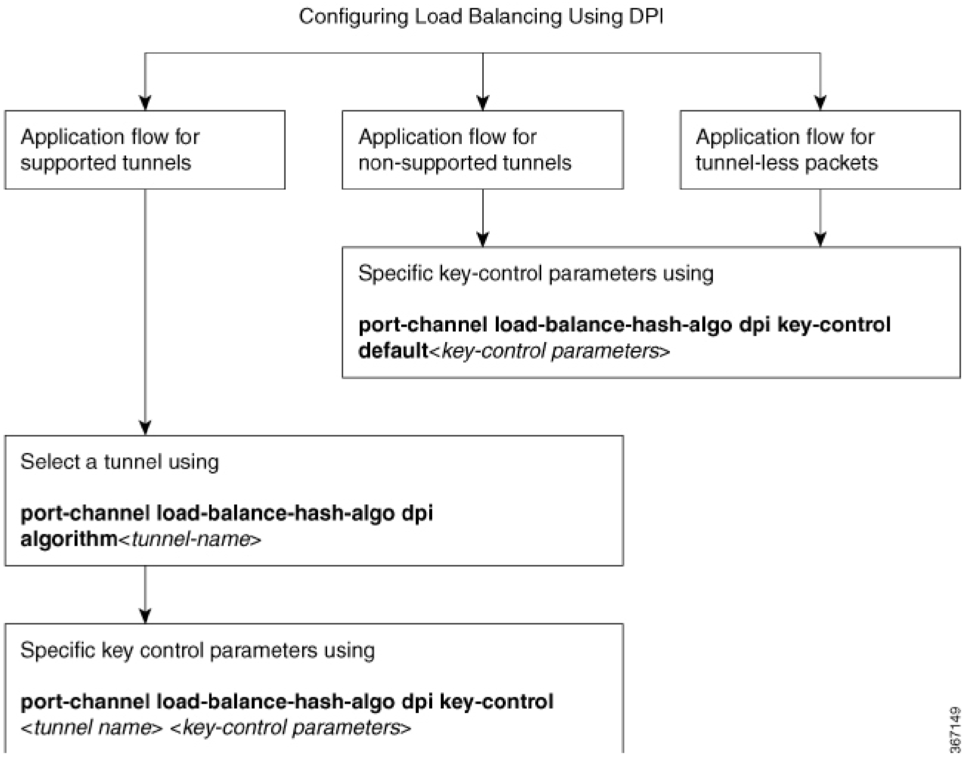
## Support for Tunnel and Tunnel-Less Packets

The DPI algorithm is supported for the following tunnels:

- GRE
- IPsec
- IPinIP
- VxLAN
- In addition to supporting the above mentioned tunnels, DPI can also be performed for tunnel-less packets using **port-channel load-balance-hash-algo dpi key-control default** command.

  When you configure load balancing using DPI you can specify a specific tunnel using the **port-channel load-balance-hash-algo dpi algorithm <tunnel-name>** command. If you prefer to configure DPI for all the tunnels, use the **port-channel load-balance-hash-algo dpi algorithm** command without a tunnel name. This configures DPI for all the tunnels and port-channels.

*Figure 4: Configuring Load Balancing Using DPI*


Configuring Load Balancing Using DPI
Application flow for supported tunnels
Application flow for non-supported tunnels
Application flow for tunnel-less packets
Specific key-control parameters using
port-channel load-balance-hash-algo dpi key-control default<key-control parameters>
Select a tunnel using
port-channel load-balance-hash-algo dpi algorithm<tunnel-name>
Specific key control parameters using
port-channel load-balance-hash-algo dpi key-control <tunnel name> <key-control parameters>
367149

# Key-Control Parameters for Hashing at Granular Level

You can configure the key-control parameters required for calculating the hash value for packets of a specific tunnel. These key-control parameters help you define load balancing at a granular level for all the active links.

| Type of Tunnel | Key-Control Parameter Set 1 | Key-Control Parameter Set 2 | Key-Control Parameter Set 3 | Key-Control Parameter 4 |
|---|---|---|---|---|
| default | outer-dst-ip<br>outer-src-dst-ip<br>outer-src-ip | ignore-outer-port<br>outer-dst-port<br>outer-src-dst-port<br>outer-src-port | | |
| tunnel-ipinip | outer-dst-ip<br>outer-src-dst-ip<br>outer-src-ip | ignore-inner-ip<br>inner-dst-ip<br>inner-src-dst-ip<br>inner-src-ip<br>inner-dst-ip<br>inner-src-dst-ip<br>inner-src-ip | ignore-inner-port<br>inner-dst-port<br>inner-src-dst-port<br>inner-src-port<br>inner-dst-port<br>inner-src-dst-port<br>inner-src-port | |

| Type of Tunnel | Key-Control Parameter Set 1 | Key-Control Parameter Set 2 | Key-Control Parameter Set 3 | Key-Control Parameter 4 |
|---|---|---|---|---|
| tunnel-gre | outer-dst-ip<br>outer-src-dst-ip<br>outer-src-ip | ignore-inner-ip<br>inner-dst-ip<br>inner-src-dst-ip<br>inner-src-ip | ignore-inner-port<br>inner-dst-port<br>inner-src-dst-port<br>inner-src-port | |
| tunnel-ipsec | ignore-outer-ip<br>outer-dst-ip<br>outer-src-dst-ip<br>outer-src-ip | | | |
| tunnel-vxlan | ignore-outer-ip<br>outer-dst-ip<br>outer-src-dst-ip<br>outer-src-ip | ignore-outer-port<br>outer-dst-port<br>outer-src-dst-port<br>outer-src-port | ignore-inner-mac<br>inner-dst-mac<br>inner-src-dst-mac<br>inner-src-mac | ignore-inner-vlan<br>inner-vlan |
| tunnel-l2tp | ignore-outer-ip<br>outer-dst-ip<br>outer-src-dst-ip<br>outer-src-ip | ignore-outer-port<br>outer-dst-port<br>outer-src-dst-port<br>outer-src-port | ignore-inner-ip<br>inner-dst-ip<br>inner-src-dst-ip<br>inner-src-ip | ignore-inner-port<br>inner-dst-port<br>inner-src-dst-port<br>inner-src-port |

# Default Key-Control Parameters for Tunnels

It is optional to have key-control parameters configured for the tunnels or tunnel-less traffic. If key-control parameters are not configured, default key-control parameters are applied for both tunnel and tunnel-less traffic.

*Table 6:*

| Type of Tunnel | Default Key-Control Parameter Set 1 | Default Key-Control Parameter Set 2 | Default Key-Control Parameter Set 3 | Default Key-Control Parameter Set 4 |
|---|---|---|---|---|
| default | outer-dst-ip | ignore-outer-port | | |
| tunnel-ipinip | outer-dst-ip | ignore-inner-ip | ignore-inner-port | |
| tunnel-gre | outer-src-dst-ip | ignore-inner-ip | ignore-inner-port | |
| tunnel-ipsec | ignore-outer-ip | | | |
| tunnel-vxlan | ignore-outer-ip | ignore-outer-port | ignore-inner-mac | ignore-inner-vlan |
| tunnel-l2tp | ignore-outer-ip | ignore-outer-port | ignore-inner-ip | ignore-inner-port |

# How to Configure Load Balancing Using Deep Packet Inspection

## Configuring Load Balancing Using Deep Packet Inspection for Tunnel-Based Flow

```
enable
configure terminal
port-channel load-balance-hash-algo dpi algorithm <tunnelname>
port-channel load-balance-hash-algo dpi key-control <tunnel-name> <key-control variables>
end
```

### Examples for Configuring Load Balancing Using for Tunnel-Based Flow

#### Example: Configuring DPI for IPinIP Tunnel

```
enable
configure terminal
(config)# port-channel load-balance-hash-algorithm dpi tunnel-ipinip
```

#### Example: Configuring DPI for IPinIP Tunnel with Key-Control Parameter

```
enable
configure terminal
(config)# port-channel load-balance-hash-algorithm dpi keycontrol tunnel-ipinip
outer-src-dst-ip ignore-inner-ip
ignore-inner-port
```

#### Example: Configuring DPI for GRE Tunnel

```
enable
configure terminal
port-channel load-balance-hash-algorithm dpi tunnel-gre
end
```

#### Example: Configuring DPI for GRE Tunnel with the Key-Control Parameter

```
enable
configure terminal
port-channel load-balance-hash-algorithm dpi key-control tunnel-gre outer-src-dst-ip
ignore-inner-ip ignore-inner-
port
end
```

#### Example: Configuring DPI for IPsec Tunnel

```
enable
configure terminal
port-channel load-balance-hash-algorithm dpi tunnel-ipsec
end
```

#### Example: Configuring DPI for IPsec Tunnel with the Key-Control Parameter

```
enable
configure terminal
port-channel load-balance-hash-algorithm dpi key-control keycontrol tunnel-ipsec
ignore-outer-ip
end
```

# How to Configure Load Balancing Using Deep Packet Inspection

## Configuring Load Balancing Using Deep Packet Inspection for Tunnel-Less Packets

```
enable
configure terminal
port-channel load-balance-hash-algorithm dpi key-control default  <key-control variables>
end
```

### Examples for Configuring Load Balancing Using for Tunnel-Less Packets

#### Example: Configuring DPI for Load Balancing Tunnel-Less Packets

```
enable
configure terminal
port-channel load-balance-hash-algorithm dpi key-control default  outer-src-dst-ip
ignore-outer-port
end
```

## Verifying DPI for Tunnel-Based and Tunnel-Less Packets

Use the **show etherchannel load-balancing** command to verify that load balancing configuration is successful

```
Router# show etherchannel load-balancing
EtherChannel Load-Balancing Method:
Global LB Method: flow-based
LB Algo type: Deep packet inspection
Enabled Tunnel Types and Associated Key-Controls
tunnel-ipinip outer-src-dst-ip inner-src-dst-ip innersrc-
dst-port
default outer-src-dst-ip ignore-outer-port
Port-Channel: LB Method
Port-channel1 : flow-based (Deep
packet inspection)
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Load Balancing with DPI Algorithm

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 7: Feature Information for Load Balancing Using DPI Algorithm*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Load Balancing Application Flows Using Deep Packet Inspection | Cisco IOS XE Gibraltar 16.10.1. | The Deep Packet Inspection (DPI)<br>helps in identification of application flows to facilitate detailed inspection of packets. The DPI algorithm deeply inspects the packets and therefore helps the service provider identify efficient ways to share bandwidth among parallel Ethernet interfaces.<br>The following commands were modified:<br>port-channel load-balance-hash-algorithm dpi algorithm. .<br>port-channel load-balance-hash-algorithm dpi key-control. . |

CHAPTER 7

# Configuring Epochs

This document contains information about and instructions for configuring epochs for Cisco Express Forwarding tables. You can use this functionality to clear and rebuild Cisco Express Forwarding tables for consistency purposes without the loss of table information.

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

## Prerequisites for Epochs for CEF Tables

Cisco Express Forwarding must be up and running on the router or switch for you to configure epochs for Cisco Express Forwarding Forwarding Information Base (FIB) and adjacency tables.

# Information About Epochs for CEF Tables

Tasks for configuring epochs for Cisco Express Forwarding FIB tables were introduced with the Nonstop Forwarding Enhanced FIB Refresh feature.

Before you configure epochs for Cisco Express Forwarding tables, you should understand the following:

(See the Nonstop Forwarding Enhanced FIB Refresh, on page 70 for an explanation of the term "epoch.")

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features you can configure, refer to the Additional References, on page 77.

## Cisco Platform Support for Central CEF and dCEF

Cisco Express Forwarding is enable by default on the Cisco ASR 1000 Series Aggregation Services Routers.

To find out if Cisco Express Forwarding is enabled on your platform, enter the **show ip cef**command. If Cisco Express Forwarding is enabled, you receive output that looks like this:

```
Router# show ip cef
Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet2/1/0
[...]
```

If Cisco Express Forwarding is not enabled on your platform, the output for the **show ip cef**command looks like this:

```
Router# show ip cef
%CEF not running
```

If Cisco Express Forwarding is not enabled on your platform, use the **ip cef**command to enable (central) Cisco Express Forwarding or the **ip cef distributed** command to enable Distributed Cisco Express Forwarding.

## Nonstop Forwarding Enhanced FIB Refresh

Networks must be configured to minimize traffic disruption and offer the most uptime possible. The Nonstop Forwarding (NSF) Enhanced FIB Refresh feature enables users to continue forwarding IP traffic while Cisco Express Forwarding database tables are being rebuilt. IP forwarding on the router is therefore uninterrupted.

NSF Enhanced FIB Refresh provides for the continuation of Cisco Express Forwarding forwarding by tracking epochs. The term "epoch" refers to a period of time. A new epoch for a Cisco Express Forwarding table begins when a table rebuild is initiated. The time after this instant is in an epoch different from the time before, and the different epochs are numbered between 0 and 255. Through the use of epochs, the software can distinguish between old and new forwarding information in the same database structure and can retain the old Cisco Express Forwarding database table while the software builds a new table. This is called epoch tracking and it allows Cisco Express Forwarding forwarding to continue uninterrupted while new Cisco Express Forwarding tables are being constructed, and it makes possible a seamless switchover when the new table becomes active.

# Epoch Numbering for CEF FIB and Adjacency Tables

A new epoch for a Cisco Express Forwarding table begins when a table rebuild is initiated. The time after this instant is in an epoch different from the time before. The first epoch is numbered 0, and it begins when the Cisco Express Forwarding table is created. The epoch number increases by 1 for each new revision of the Cisco Express Forwarding table until the epoch number reaches 255. The next epoch after 255 is 0. A new epoch cannot begin if any table entries remain from the last time the epoch number was used. The epoch number for a given table is the same for each instance of the table (for example, on each RP and on each line card where distributed Cisco Express Forwarding is active).

Each entry added to a FIB table or the adjacency table has a new field that records the current epoch for that table at the time the entry was added. When an entry is modified, the epoch of the entry is updated to record the table's current epoch. A record is kept of how many entries exist from each epoch. The epoch number cannot be incremented if any existing entries have the same epoch number as the next epoch value.

When the routing protocols signal that they have converged, all FIB and adjacency entries that have epoch numbers older than the current epoch number are removed from the FIB and adjacency tables.

When you need a Cisco Express Forwarding table to be rebuilt, the epoch number for that table is incremented, and the table is rebuilt in place. When rebuilding is complete, "stale" entries are removed from the table. You can increment the epoch of a single table or multiple tables at the same time when you enter the **clear ip cef epoch** [**all-vrfs** | **full** | **vrf**[*table*]] command. See the When to Refresh the CEF or Adjacency Tables section for information on when you might need to rebuild a Cisco Express Forwarding table.

When you display information from a Cisco Express Forwarding table (for example, with the **show ip cef epoch**command), the table epoch is shown in the summary table. When detailed information is displayed for each table entry, the epoch number of each entry is shown.

# Epoch Synchronization Between the RP and Line Cards

When FIB or adjacency entries are distributed from the central tables on the RP, the updates contain the epoch of the entry, ensuring that the distinction between old and new entries is maintained in distributed systems.

When a table is initialized on a line card, the current epoch of the table on the RP is sent to the line card. When the epoch is incremented on the RP, an event indicating that a new epoch has begun is sent to each line card.

# Epoch Numbering for Routers That Support HA

In a router that supports high availability (HA), the epoch numbers for all Cisco Express Forwarding tables are incremented when an RP transitions from standby mode to active. After switchover, the active secondary RP initially has FIB and adjacency databases that are the same as those of the primary RP. When the epoch number for each table is incremented, all existing entries are considered stale. However, forwarding continues as normal. As the routing protocols start to repopulate the FIB and adjacency databases, existing and new entries receive the new epoch number, indicating that the entries have been refreshed.

# When to Refresh the CEF or Adjacency Tables

You refresh or rebuild the Cisco Express Forwarding or adjacency tables when the tables contain inconsistencies.

Cisco ASR 1000 Series Routers support distributed Cisco Express Forwarding, in which line cards make forwarding decisions based on stored copies of the same FIB and adjacency tables that are found on the RP. The tables on the line cards and the RP must remain synchronized.

Inconsistencies occur when forwarding information (a prefix) is missing on a line card, or the next-hop IP address on the line card is not the same as the next-hop IP address on the RP. Because updates to the RP and line card databases are not synchronous, fleeting inconsistencies can result.

Cisco Express Forwarding consistency checkers detect when forwarding information on the line cards and the RP lose synchronization. For more information on consistency checkers, see the "Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards" module.

# How to Configure Epochs

This section contains instructions on how to configure epochs for Cisco Express Forwarding tables. Perform the following tasks to begin new epochs and increment the epoch number of the adjacency and Cisco Express Forwarding tables:

## Incrementing the Epoch Number of the Adjacency Table

Perform the following task to begin a new epoch and increment the epoch number of the adjacency table.

Use this task when you need to rebuild the adjacency table. A new adjacency table might be required because you need to remove inconsistencies from the table.

### SUMMARY STEPS

1. **enable**
2. **show adjacency summary**
3. **clear adjacency table**
4. **show adjacency summary**
5. **disable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show adjacency summary**<br>**Example:**<br>`Router# show adjacency summary` | Displays a summary of the information about the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table. |
| **Step 3** | **clear adjacency table**<br>**Example:**<br>`Router# clear adjacency table` | Begins a new epoch and increments the epoch number of the adjacency table. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **show adjacency summary**<br>**Example:**<br>`Router# show adjacency summary` | Displays a summary of the information about the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table. |
| **Step 5** | **disable**<br>**Example:**<br>`Router# disable` | Exits to user EXEC mode. |

# Incrementing the Epoch Number of One or All CEF Tables

Perform the following task to begin a new epoch and increment the epoch number of one or all of the Cisco Express Forwarding tables.

Use the **clear cef table** command when you want to rebuild a Cisco Express Forwarding table. This command clear 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.

### SUMMARY STEPS

1. **enable**
2. **show ip cef epoch**
3. **clear cef table** {**ipv4** | **ipv6**} [**vrf** {*vrf-name*| *****}]
4. **show ip cef epoch**
5. **disable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show ip cef epoch**<br>**Example:**<br>`Router# show ip cef epoch` | Displays entries in the FIB or displays a summary of the FIB.<br>• The **epoch** keyword displays the table epochs of the FIB tables. |
| **Step 3** | **clear cef table** {**ipv4** \| **ipv6**} [**vrf** {*vrf-name*\| *****}]<br>**Example:** | Clears the Cisco Express Forwarding tables.<br>• The **ipv4** keyword specifies the Cisco Express Forwarding tables for IPv4 addresses. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# clear cef table ipv4` | - The **ipv6** keyword specifies the Cisco Express Forwarding tables for IPv6 addresses.<br>- The **vrf** keyword specifies all VPN routing and forwarding (VRF) instance tables or a specific VRF table for an IPv4 or IPv6 address.<br>- The *vrf-name* argument specifies the specific VRF table for IPv4 or IPv6 addresses.<br>- The ***** (asterisk) keyword specifies all the VRF tables for IPv4 or IPv6 addresses.<br>**Note** This command also increments the table epoch, updates the tables, and distributes the updated information to the line cards. |
| **Step 4** | **show ip cef epoch**<br>**Example:**<br>`Router# show ip cef epoch` | Displays entries in the FIB or displays a summary of the FIB.<br>- The **epoch** keyword displays the epochs of the FIB tables. |
| **Step 5** | **disable**<br>**Example:**<br>`Router# disable` | Exits to user EXEC mode. |

# Verifying Epoch Information

Perform the following task to verify epoch information for Cisco Express Forwarding and adjacency tables.

## SUMMARY STEPS

1. **enable**
2. **show adjacency summary detail**
3. **show adjacency summary**
4. **show ip cef epoch**
5. **disable**

## DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. For example:

**Example:**

```
Router> enable
```

Enter your password if prompted.

**Step 2** **show adjacency summary detail**

Use this command to verify that the epoch number is displayed for each entry in the adjacency table as you expect. For example:

**Example:**

```
Router# show adjacency detail
Protocol Interface                 Address
IP       Serial2/0/1:1           point2point(7)
                                   0 packets, 0 bytes
                                   0F000800
                                   CEF   expires: 00:02:09
                                         refresh: 00:00:09
                                   Epoch: 14 ! ====> Epoch number
IP       Serial2/1/1:1           point2point(7)
                                   0 packets, 0 bytes
                                   0F000800
                                   CEF   expires: 00:02:09
                                         refresh: 00:00:09
                                   Epoch: 14 ! ====> Epoch number
```

The epoch number is displayed for each entry in the adjacency table. In this example, the epoch number of each entry is 14.

**Step 3** **show adjacency summary**

Use this command to verify that the epoch number for each adjacency in the adjacency table is as you expect. For example:

**Example:**

```
Router# show adjacency summary
Adjacency Table has 2 adjacencies
  Table epoch: 14 (2 entries at this epoch)

Interface                 Adjacency Count
 Serial2/0/1:1             1
 Serial2/1/1:1             1
```

Use the epoch information in the summary section to verify that the epoch number for each adjacency in the adjacency table is as expected. The epoch number is 14 in this example, the same as the epoch number displayed in the **show adjacency detail** command in the previous step.

**Step 4** **show ip cef epoch**

Use this command to verify that Cisco Express Forwarding information in all FIB tables is as you expect. In the following example, Cisco Express Forwarding epoch information is verified for all FIB tables:

**Example:**

```
Router# show ip cef epoch
CEF epoch information:

Table: Default-table
  Table epoch: 77 (19 entries at this epoch)
```

**Step 5** **disable**

Use this command to exit to user EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

# Configuration Examples for Epochs

## Example Incrementing the Epoch Number of the Adjacency Table

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

```
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 adjacency table
```

After clearing:

```
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)
```

## Example Incrementing the Epoch Number of One or All CEF Tables

The following example shows how to begin a new epoch and increment the epoch number of all Cisco Express Forwarding tables for the IPv6 address family:

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

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

```
Router# show ip cef epoch
Table: Default-table
  Database epoch: 3 (43 entries at this epoch)
```

After clearing:

```
Router# clear cef table ipv4
Router# show ip cef epoch
Table: Default-table
  Database epoch: 4 (43 entries at this epoch)
```

The following examples shows how to clear Cisco Express Forwarding tables for all VRF tables in the IPv4 address family. This examples shows sample output with Cisco Express Forwarding debugging (**debug cef**command) 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.
Trying 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,
flags 00420005
06:56:06: FIBtable: IPv4: Adding route for 0.0.0.0/0 but route already exists.
Trying modify.
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Description of Cisco Express Forwarding commands | *Cisco IOS IP Switching Command Reference* |
| Description of Cisco Express Forwarding IPv6 commands | *Cisco IOS IPv6 Command Reference* |

| Related Topic | Document Title |
|---|---|
| Information on MFI enhancements | MPLS Infrastructure Changes: Introduction of MFI and Removal of MPLS LSC and LC-ATM Features |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Configuring Epochs

*Table 8: Feature Information for Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| Nonstop Forwarding Enhanced FIB Refresh | Cisco IOS XE Release 2.1 | This feature allows you to clear the forwarding table on demand and to continue forwarding through the use of the old entries in the table while the new forwarding table is being built.<br>In Cisco IOS XE, Release 2, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Router.<br>No commands were introduced or modified for this feature. |

# Glossary

**adjacency** --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

**Cisco Express Forwarding** --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

**distributed Cisco Express Forwarding** --A mode of Cisco Express Forwarding operation in which line cards maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Processor of involvement in the switching operation.

**FIB** --forwarding information base. A component of Cisco Express Forwarding that is conceptually similar to a routing table or information base. The router uses the FIB lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

**LIB** --label information base. A database used by a label switch router (LSR) to store labels learned from other LSRs, as well as labels assigned by the local LSR.

**line card** --A general term for an interface processor that can be used in various Cisco products.

**prefix** --The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are the network bits. For example, 1.0.0.0/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 10.0.

**RIB** --Routing Information Base. A central repository of routes that contains Layer 3 reachability information and destination IP addresses or prefixes. The RIB is also known as the routing table.

**RP** --Route Processor. The processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a supervisory processor.

CHAPTER 8

# Configuring CEF Consistency Checkers

This module contains information about and instructions for configuring Cisco Express Forwarding (formerly known as CEF) consistency checkers. Cisco Express Forwarding consistency checkers enable you to find any database inconsistencies, such as an IP prefix missing from a line card or a Route Processor (RP). You can investigate and resolve the inconsistency by examining the associated Cisco Express Forwarding system error messages and by using Cisco Express Forwarding **debug** and **show** commands.

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks—those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

## Prerequisites for CEF Consistency Checkers

Cisco Express Forwarding must be up and running on the networking device before you can configure Cisco Express Forwarding consistency checkers.

# Restrictions for CEF Consistency Checkers

The Cisco Express Forwarding consistency checkers—lc-detect, scan-lc-rp—apply only to devices that have distributed Cisco Express Forwarding enabled.

# Information About CEF Consistency Checkers

## Cisco Platform Support for CEF and dCEF

Cisco Express Forwarding is enabled by default on the Cisco ASR 1000 Series Aggregation Services Routers.

To find out if Cisco Express Forwarding is enabled on your platform, enter the **show ip cef** command. If Cisco Express Forwarding is enabled, you will see the following output:

```
Device# show ip cef

Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet2/1/0
[...]
```

If Cisco Express Forwarding is not enabled on your platform, you will see the following output for the **show ip cef** command:

```
Device# show ip cef

%CEF not running
```

If Cisco Express Forwarding is not enabled on your platform, use the **ip cef** command to enable Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

## CEF Consistency Checker Types

Cisco Express Forwarding uses the routing information that is retrieved from the Routing Information Base (RIB), the Route Processor (RP), and the line card databases to perform express forwarding. Updating these databases may result in incosistencies because the distribution mechanism for these databases is asynchronous. Inconsistencies caused by asynchronous database distribution are of the following types:

- Missing information, such as a particular prefix, on a line card
- Different information, such as different next-hop IP addresses, on the line card

Cisco Express Forwarding supports passive and active consistency checkers that run independently to uncover these forwarding inconsistencies. The following table describes the consistency checkers and indicates whether the checker operates on the RP or the line card.

*Table 9: Types of Cisco Express Forwarding Consistency Checkers*

| Checker Type | Operates On | Description |
|---|---|---|
| lc-detect | Line card | (Distributed Cisco Express Forwarding only) Detects missing prefixes on the line card. The information is confirmed by the RP.<br>Retrieves IP prefixes found missing from the line card forwarding information base (FIB) table. If IP prefixes are missing, the line card cannot forward packets for the corresponding addresses. The consistency checker then sends IP prefixes to the RP for confirmation. If the RP finds that it has the relevant entry, an inconsistency is detected, and an error message is displayed. Finally, the RP sends a signal back to the line card confirming that the IP prefix is an inconsistency. |
| scan-lc-rp | Line card | Distributed Cisco Express Forwarding only looks through the FIB table for a configurable time period and sends the next *x* prefixes to the RP. The RP does an exact lookup in its FIB table. If the RP finds that the prefix is missing, the RP reports an inconsistency. Finally, the RP sends a signal back to the line card for confirmation.<br>The time period and the number of prefixes sent are configured with the **cef table consistency-check** command. |
| scan-rp-lc | Route Processor | (Distributed Cisco Express Forwarding only) Looks through the RP FIB table for a configurable time period and sends the next *x* prefixes to the line card. (This action is opposite to the one that the scan-lc-rp checker performs.) The line card does an exact lookup in the FIB table. If the line card finds the prefix missing, the line card reports an inconsistency and signals the RP for confirmation.<br>The time period and the number of prefixes sent are configured with the **cef table consistency-check** command. |
| scan-rib-ios | Route Processor | Compares the Routing Information Base (RIB) to the FIB table and provides the number of entries missing from the FIB table. |
| scan-ios-rib | Route Processor | Compares the FIB table to the RIB and provides the number of entries missing from the RIB. |

Cisco Express Forwarding consistency checkers are disabled by default. Console errors are disabled by default.

If you find a database inconsistency, such as an IP prefix missing from a line card or an RP, you can investigate and resolve the inconsistency by examining the Cisco Express Forwarding system error messages and by using Cisco Express Forwarding **debug** and **show** commands.

For Cisco Express Forwarding consistency checker system error messages, see the System Messages for Cisco IOS XE Software.

# How to Configure CEF Consistency Checkers

## Enabling CEF Consistency Checkers

Perform the following task to enable Cisco Express Forwarding consistency checkers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cef table consistency-check** {**ipv4** | **ipv6**} [**auto-repair** [**delay** *seconds* [**holddown** *seconds*] | **holddown** *seconds*] | **data-checking** | **error-message** | **type** {**lc-detect** | **scan-lc-rp** | **scan-rp-lc** | **scan-rib-ios** | **scan-ios-rib**} [**count** *count-number* [**period** *seconds*] | **period** *seconds*]]
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cef table consistency-check** {**ipv4** \| **ipv6**} [**auto-repair** [**delay** *seconds* [**holddown** *seconds*] \| **holddown** *seconds*] \| **data-checking** \| **error-message** \| **type** {**lc-detect** \| **scan-lc-rp** \| **scan-rp-lc** \| **scan-rib-ios** \| **scan-ios-rib**} [**count** *count-number* [**period** *seconds*] \| **period** *seconds*]]<br>**Example:**<br>`Device(config)# cef table consistency-check ipv4 scan-rib-ios count 100 period 60` | Enables Cisco Express Forwarding table consistency checker types and parameters.<br>• The **ipv4** keyword checks IPv4 addresses.<br>• The **ipv6** keyword checks IPv6 addresses.<br>• The **auto-repair** keyword 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 reset the auto-repair settings to a 10-second delay and 300-second holddown time.<br>• The **delay** *seconds* keyword-argument pair specifies how long the consistency checker waits to fix an inconsistency. The valid range is from10 to 300 seconds. The default delay value is 10 seconds<br>• The **holddown** *seconds* keyword and argument pair specifies how long the consistency checker waits to |

| | Command or Action | Purpose |
|---|---|---|
| | | reenable auto repair after auto repair runs. The valid range is from 300 to 3000 seconds. The default delay value is 300 seconds.<br>• The **data-checking** keyword enables the consistency checker data-checking utility. By default, this function is disabled.<br>• The **error-message** keyword enables the consistency checker to generate an error message when it detects an inconsistency. By default, this function is disabled.<br>• The **type** keyword indicates the type of consistency check that can be enabled.<br>• The **lc-detect** keyword enables the line card to detect a missing prefix, which is confirmed by the Route Processor (RP).<br>• The **scan-lc-rp** keyword performs a passive scan check of tables on the line card.<br>• The **scan-rp-lc** keyword enables a passive scan check of tables on the RP.<br>• The **scan-rib-ios** keyword compares the Routing Information Base (RIB) to the forwarding information base (FIB) and provides the number of entries missing from the FIB table.<br>• The **scan-ios-rib** keyword compares the FIB table to the RIB and provides the number of entries missing from the RIB.<br>• The **count** *number* keyword-argument pair specifies the maximum number of prefixes to check per scan. The valid range is from 2 to 10000.<br>• The **period** *seconds* keyword-argument pair specifies the time during which updates for a candidate prefix are ignored as inconsistencies. The valid range is from 30 to 3600 seconds. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

# Displaying and Clearing Table Inconsistencies

Perform the following task to display and clear Cisco Express Forwarding table inconsistency records found by the lc-detect, scan-rp-lc, scan-lc-rp, scan-rib-ios, and scan-ios-rib detection mechanisms.

### SUMMARY STEPS

1. **enable**
2. **test cef table consistency** [**detail**]
3. **clear ip cef inconsistency**
4. **clear cef linecard** [*slot-number*] [**adjacency** | **interface** | **prefix**]
5. **show cef table consistency-check**
6. **disable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **test cef table consistency** [**detail**]<br>**Example:**<br>`Device#  test cef table consistency` | Use this command to test the Cisco Express Forwarding forwarding information base (FIB) for prefix consistency. |
| **Step 3** | **clear ip cef inconsistency**<br>**Example:**<br>`Device# clear ip cef inconsistency` | Use this command to clear the Cisco Express Forwarding inconsistency statistics and records found by Cisco Express Forwarding consistency checkers. |
| **Step 4** | **clear cef linecard** [*slot-number*] [**adjacency** \| **interface** \| **prefix**]<br>**Example:**<br>`Device# clear cef linecard` | Use this command to clear Cisco Express Forwarding information from line cards. |
| **Step 5** | **show cef table consistency-check**<br>**Example:**<br>`Device# show cef table consistency-check` | Use this command to verify the status of Cisco Express Forwarding consistency checkers in the FIB. |
| **Step 6** | **disable**<br>**Example:**<br>`Device# disable` | Use this command to exit to user EXEC mode. |

# Configuration Examples for CEF Consistency Checkers

## Example: Enabling CEF Consistency Checkers

The following example shows how to enable the scan-rp Cisco Express Forwarding consistency checker.

```
Device> enable
Device# configure terminal
Device(config)# cef table consistency-check scan-rp-lc count 225 period 3600
Device(config)# end
```

**Note** The Route Processor (RP) is configured to send 3600 prefixes to the line cards every 225 seconds.

## Example: Displaying and Clearing Table Inconsistencies

The following example shows how to test the Cisco Express Forwarding FIB for prefix consistency:

```
Device# test cef table consistency detail
```

The following is sample output from the **test cef table consistency detail** command:

```
Device# 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
```

The output of this command shows that no IPv4 inconsistencies were found and five (5) IPv6 inconsistencies were found. The output also shows how many prefixes were checked by the FIB and the linecards and how many prefixes were missing, if any.

The following is sample output from the **show cef table consistency-check** command:

```
Device# 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
```

The output of this command shows that two full scans are enabled, and at every 60 seconds, 1000 prefixes are checked. It also shows that the auto-repair function is enabled with the default settings of a 10-second delay and a 300-second holddown time. In this example, no inconsistencies were found.

# Additional References for CEF Consistency Checkers

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Master Commands List, All Releases |
| Cisco Express Forwarding Commands | *Cisco IOS IP Switching Command Reference* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for CEF Consistency Checkers

*Table 10: Feature Information for CEF Consistency Checkers*

| Feature Name | Releases | Feature Information |
|---|---|---|
| This table is intentionally left blank because no features were introduced or modified in Cisco IOS XE Release 2.1 or later. This table will be updated when feature information is added to this module. | — | — |

# Glossary

**adjacency**—A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

Cisco **Cisco Express Forwarding**—A Layer 3 switching technology. Cisco Express Forwarding can also refer to a central Cisco Express Forwarding mode, one of two modes of the Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor (RP) to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of the Cisco Express Forwarding operation.

**distributed Cisco Express Forwarding**—A mode of Cisco Express Forwarding switching in which line cards maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform express forwarding between port adapters; this relieves the Route Processor from any involvement in the switching operation.

**FIB**—forwarding information base. A component of Cisco Express Forwarding that is conceptually similar to a routing table or information base. The router uses the FIB lookup table to make destination-based switching decisions during the Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

**IPC**—interprocess communication. The mechanism that enables the distribution of Cisco Express Forwarding tables from the RP to the line card when the router is operating in distributed Cisco Express Forwarding mode.

**LIB**—label information base. A database used by a label switch router (LSR) to store labels learned from other LSRs, as well as labels assigned by the local LSR.

**line card**—A general term for an interface processor that can be used in various Cisco products.

**MPLS**—Multiprotocol Label Switching. An industry standard for the forwarding of packets along normal routing paths (sometimes called MPLS hop-by-hop forwarding).

**prefix**—The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are network bits. For example, 192.0.2.1/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 192.0.

**RIB**—Routing Information Base. A central repository of routes that contains Layer 3 reachability information and destination IP addresses or prefixes. The RIB is also known as the routing table.

**RP**—Route Processor. The processor module that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a supervisory processor.

**VPN**—Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** —A Virtual Private Network (VPN) routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a Provider Edge router.

CHAPTER 9

# Configuring CEF Network Accounting

This module contains information about and instructions for configuring network accounting for Cisco Express Forwarding. Accounting produces the statistics that enable you to better understand Cisco Express Forwarding patterns in your network. For example, you might want to find out the number of packets and bytes switched to a destination or the number of packets switched through a destination.

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

## Prerequisites for CEF Network Accounting

Cisco Express Forwarding must be up and running on the networking device before you can configure network accounting for Cisco Express Forwarding. See the Cisco Platform Support for Central CEF and dCEF section for information on how to determine if Cisco Express Forwarding is enabled on your networking device.

# Information About CEF Network Accounting

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features that you can configure, go to the Additional References, on page 109.

## Cisco Platform Support for Central CEF and dCEF

Cisco Express Forwarding is enabled by default on most Cisco platforms running Cisco IOS software Release 12.0 or later. When Cisco Express Forwarding is enabled on a router, the Route Processor (RP) performs the express forwarding.

To find out if Cisco Express Forwarding is enabled on your platform, enter the **show ip cef**command. If Cisco Express Forwarding is enabled, you receive output that looks like this:

```
Router# show ip cef
Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet6/1
[...]
```

If Cisco Express Forwarding is not enabled on your platform, the output for the **show ip cef**command looks like this:

```
Router# show ip cef
%CEF not running
```

Distributed Cisco Express Forwarding is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When distributed Cisco Express Forwarding is enabled on your platform, the line cards perform the express forwarding.

If Cisco Express Forwarding is not enabled on your platform, use the **ip cef**command to enable (central) Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

## Traffic Matrix Statistics

The traffic matrix statistics (TMS) feature allows an administrator to gather the following data:

- The number of packets and number of bytes that travel across the backbone from internal and external sources. The counts of packets and bytes are called TMS and are useful for determining how much traffic a backbone handles. You can analyze TMS using the following methods:
    - Collecting and viewing TMS through the application of the Network Data Analyzer (NDA)
    - Reading the TMS that reside on the backbone router
- The neighbor autonomous systems of a Border Gateway Protocol (BGP) destination. You can view these systems by reading the tmasinfo_ascii file on the backbone router.

The following sections explain how to collect and view the TMS using the command-line interface (CLI) and the NDA. For detailed instructions on using the NDA, see the Network Data Analyzer Installation and User Guide .

# TMS and CEF Nonrecursive Accounting

TMS enables an administrator to capture and analyze data on traffic entering a backbone that is running BGP. The TMS feature also allows an administrator to determine the neighbor autonomous systems of a BGP destination. TMS are counted during packet forwarding by Cisco Express Forwarding nonrecursive accounting.

By enabling a backbone router to gather TMS, you can determine the amount of traffic that enters the backbone from sites outside of the backbone. You can also determine the amount of traffic that is generated within the backbone. This information helps you optimize and manage traffic across the backbone.

The following paragraphs explain how Cisco Express Forwarding nonrecursive accounting aggregates packet statistics for Interior Gateway Protocol (IGP) routes and their dependent BGP routes.

A BGP network deployed by a service provider might have the following components:

- IGP routes that describe the next hop to which traffic should be sent
- BGP routes that specify an intermediate address to which traffic should be sent

The intermediate address specified for the BGP route might be several hops away from the provider edge (PE) router. The next hop for the BGP route is the next hop for the intermediate address of the BGP route. The BGP route is called recursive, because it points through an intermediate address to an IGP route that provides the next hop for forwarding. However, a route lookup results in a next hop that is not directly reachable, as is the case with the BGP route’s intermediate address. A recursive lookup to an IGP route is used to decide how to reach the indirect next hop.

Cisco Express Forwarding represents IGP routes as nonrecursive entries and BGP routes as recursive entries that resolve through nonrecursive entries.

Cisco Express Forwarding nonrecursive accounting counts the packets for all of the Cisco Express Forwarding recursive entries (from BGP routes) that resolve through a Cisco Express Forwarding nonrecursive entry and the packets for the nonrecursive entry (from IGP routes). The number of packets is totalled in one location.

The packets forwarded based on a nonrecursive Cisco Express Forwarding entry can be split into two bins based on whether the input interface of the backbone router is configured as internal or external. Thus, all packets that arrive on external interfaces (external to the region of interest) and are forwarded based on a given IGP route (either directly or through a recursive BGP route) are counted together.

The following example shows how Cisco Express Forwarding nonrecursive accounting counts packets when BGP routes resolve to one IGP route and when they do not.

A multiaccess network access point (NAP) has BGP routes referring to hosts on the NAP network.

- If the network is advertised as a single IGP route, all of the BGP routes to the various hosts at that NAP resolve to a single IGP route. Cisco Express Forwarding nonrecursive accounting counts the number of packets sent to all BGP destinations.
- If a network administrator instead advertises individual host routes from the NAP network to the IGP, Cisco Express Forwarding nonrecursive accounting counts packets to those hosts separately.

# How Backbone Routers Collect TMS

You can determine the amount of traffic that enters the backbone from sites outside of the backbone if you enable a backbone router to gather TMS. You can also determine the amount of traffic that is generated within the backbone. This information helps you optimize and manage traffic across the backbone. The figures below help illustrate the traffic statistics you can gather using TMS.

The figure below shows a sample network with backbone routers and links. The traffic that travels through the backbone is the area of interest for TMS collection. TMS are collected during packet forwarding. The backbone is represented by the darkly shaded routers and bold links. The lighter shaded and unshaded routers are outside the backbone.

The figure below shows an exploded view of the backbone router that links the Los Angeles point of presence (POP) in the figure above to the Atlanta POP. The bold line represents the backbone link going to the Atlanta POP.

The figure below shows the following types of traffic that travel through the backbone router:

- The dotted line marked A represents traffic entering the backbone from a router that is not part of the backbone. This is called external traffic.
- The dotted lines marked B and D represent traffic that is exiting the backbone. This is called internal traffic.
- The dotted line marked C represents traffic that is not using the backbone and is not of interest to TMS.

You can determine the amount of traffic the backbone handles by enabling a backbone router to track the number of packets and bytes that travel through the backbone router. You can separate the traffic into the categories "internal" and "external." You separate the traffic by designating incoming interfaces on the backbone router as internal or external.

Once you enable a backbone router to collect TMS, the router starts counters, which dynamically update when network traffic passes through the backbone router. You can retrieve a snapshot of the TMS, either through a command to the backbone router or through the NDA.

External traffic (path A in the figure above) is the most important for determining the amount of traffic that travels through a backbone router. Internal traffic (paths B and D in the figure above) is useful for ensuring that you are capturing all of the TMS data. When you receive a snapshot of the TMS, the packets and bytes are displayed in internal and external categories.

# TMS Viewing Options

Once TMS are collected, you have three options for viewing the data:

This section contains the following information about the display of accounting data:

## TMS Displayed with the NDA Display Module

The NDA collects TMS from the backbone router and displays the data through the NDA Display module. The TMS can look similar to the data shown in the two figures below. The display format depends on the aggregation scheme you select. See the Network Data Analyzer Installation and User Guide for more information.

(The view of data that the NDA Display module provides is wide. Slide the scroll bar to the right and left to see all of the data. The two figures below taken together show all of the columns of data.)

## Nonrecursive Accounting Information Displayed

You can use the **show ip cef** command to display nonrecursive accounting information, including the counts of internal and external packets and bytes that have traveled through the IP prefix address/mask (in the format a.b.c.d/len) for an IGP route. Here is an example that shows 0 packets and 0 bytes of external traffic and 1144 packets and 742 bytes of internal traffic for the router with the IP address 10.102.102.102:

```
Router# show ip cef 10.102.102.102
10.102.102.10/32, version 34, epoch 0, per-destination sharing
0 packets, 0 bytes
 tag information set
  local tag: 19
 via 10.1.1.100, FastEthernet0/0/0, 0 dependencies
  next hop 10.1.1.100, FastEthernet0/0/0
  valid adjacency
  tag rewrite with FE0/0/0, 10.1.1.100, tags imposed {17}
 0 packets, 0 bytes switched through the prefix
 tmstats: external 0 packets, 0 bytes
      internal 1144 packets, 742 bytes
 30 second output rate 0 Kbits/sec
```

# Statistics in the timestats File

Before you perform the task to interpret the statistics in the tmstats_ascii file (an optional procedure described in the Interpreting the tmstats File section), you need to understand the following:

### Virtual Files on the Backbone Router

You can read TMS that reside on the backbone router and are stored in the following virtual files:

- tmstats_ascii--TMS in ASCII (human readable) format
- tmstats_binary--TMS in binary (space-efficient) format

The binary file tmstats_binary contains the same information as the ASCII file, except in a space-efficient format. You can copy this file from the router and read it with any utility that accepts files in binary format.

### tmstats File Header Description

The tmstats_ascii file header provides the address of the backbone router and information about how much time the router used to collect and export the TMS data. The header occupies one line and uses the following format:

```
VERSION 1|ADDR
<address>
|AGGREGATION
TrafficMatrix.ascii|SYSUPTIME
<seconds>|
routerUTC
<routerUTC>
|NTP
<synchronized|unsynchronized>|DURATION
<aggregateTime>
|
```

The table below describes the fields in the file header of the tmstats_ascii file.

*Table 11: Fields in tmstats_ascii File Header*

| Maximum Field Length | Field | Description |
|---|---|---|
| 10 | VERSION | File format version |

| Maximum Field Length | Field | Description |
|---|---|---|
| 21 | ADDR | The IP address of the router |
| 32 | AGGREGATION | The type of data being aggregated |
| 21 | SYSUPTIME | The time of export (in seconds) since the router booted |
| 21 | routerUTC | The time of export (in seconds) since 1900-01-01 (Coordinated Universal Time (UTC)), as determined by the router |
| 19 | NTP | An indication of whether or not the UTC of the router has been synchronized by the Network Time Protocol (NTP) with an authoritative time source, such as a radio clock or an atomic clock attached to a time server |
| 20 | DURATION | The time needed to capture the data (in seconds) (trailing \|) |

### Destination Prefix Record Description

The destination prefix record displays the internal and external packets and bytes for the IGP route and uses the following format:

```
p|
<destPrefix/Mask>
|
<creationSysUpTime>
|
<internalPackets>
|
<internalBytes>
|
<externalPackets>
|
<externalBytes>
```

The per-prefix records display information only about label switched traffic data. Label forwarding across a backbone router or switch, is based on either dynamic label switching or traffic engineered paths.

The table below describes the fields in the destination prefix record.

*Table 12: Destination Prefix Record Fields*

| Maximum Field Length | Field | Description |
|---|---|---|
| 2 | *<recordType>* | **p** means that the record represents dynamic label switching (for example, LDP) data or headend traffic engineering (TE) tunnel traffic data.<br>**t** means that the record contains TE tunnel midpoint data. |
| 19 | destPrefix/Mask | The IP prefix address/mask (in the format a.b.c.d/len) for this IGP route. |

| Maximum Field Length | Field | Description |
|---|---|---|
| 11 | creationSysUpTime | How long the system had been running when the record was first created. |
| 21 | internalPackets | Internal packet count. |
| 21 | internalBytes | Internal byte count. |
| 21 | externalPackets | External packet count. |
| 20 | externalBytes | External byte count (no trailing \|). |

### Tunnel Midpoint Record Description

The tunnel midpoint record displays the internal and external packets and bytes for the tunnel head and uses the following format:

```
t|
<headAddr><tun_id>
|
<creationSysUpTime>
|

<internalPackets>
|
<internalBytes>
|
<externalPackets>
|
<externalBytes>
```

The table below describes the fields in the tunnel midpoint record.

*Table 13: Tunnel Midpoint Record Fields*

| Maximum Field Length | Field | Description |
|---|---|---|
| 2 | *<recordType>* | **t** means that the record contains TE tunnel midpoint data. |
| 27 | headAddr<*space*>tun_id | The IP address of the tunnel head and tunnel interface number. |
| 11 | creationSysUpTime | How long the system had been running when the record was first created. |
| 21 | internalPackets | Internal packet count. |
| 21 | internalBytes | Internal byte count. |
| 21 | externalPackets | External packet count. |
| 20 | externalBytes | External byte count (no trailing \|). |

# Statistics in the tmsasinfo File

Before viewing the statistics in thetmsasinfo file (an optional procedure described in the Viewing Information in the tmsasinfo File, on page 105), you need to understand the following:

### Header Format for the tmsasinfo File

The file header provides the address of the router and indicates how much time the router used to collect and export the data. The file header uses the following format:

```
VERSION 1|ADDR
<address>
|AGGREGATION
ASList.ascii|SYSUPTIME
<seconds>|routerUTC

<routerUTC>
|DURATION
<aggregateTime>
|
```

The table below describes the fields in the file header.

*Table 14: Fields in the tmsasinfo File Header*

| Maximum Field Length | Field | Description |
|---|---|---|
| 5 | VERSION | File format version |
| 15 | ADDR | The IP address of the router |
| 20 | AGGREGATION | The type of data being aggregated |
| 10 | SYSUPTIME | The time of export (in seconds) since router booted |
| 10 | routerUTC | The time of export (in seconds) since 1900-01-01, as determined by the router |
| 10 | DURATION | The time needed to capture the data (in seconds) |

### Neighbor AS Record in the tmsasinfo File

The neighbor AS record displays the neighbor AS and the underlying prefix/mask for each BGP route. The record uses the following format:

```
<nonrecursivePrefix/Mask>
|
<AS>
|
<destinationPrefix/Mask>
```

The table below describes the fields in the neighbor AS record.

*Table 15: Neighbor AS Record Fields*

| Maximum Field Length | Field | Description |
|---|---|---|
| 18 | nonrecursivePrefix/Mask | The IP prefix address/mask (a.b.c.d/len format) for this IGP route |
| 5 | AS | The neighbor AS |
| 18 | destinationPrefix/Mask | The prefix/mask for the Forwarding Information Base (FIB) entry (typically BGP route) |

# How to Configure CEF Network Accounting

## Configuring CEF Network Accounting

Perform the following task to enable network accounting for Cisco Express Forwarding.

When you enable network accounting for Cisco Express Forwarding from the global configuration mode, accounting information is collected on the RP.

When you enable network accounting for distributed Cisco Express Forwarding from the global configuration mode, accounting information grouped by IP prefix (recursive or nonrecursive) is not sent to the RP, but is collected on the line card.

After accounting information is collected for Cisco Express Forwarding or distributed Cisco Express Forwarding, you can display the statistics using the **show ip cef** command. To verify the statistics on a line card, use the **show cef interface statistics**command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef accounting** {[**non-recursive**] [**per-prefix**] [**prefix-length**]}
4. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ip cef accounting** {[**non-recursive**] [**per-prefix**] [**prefix-length**]}<br>**Example:**<br>`Router(config)# ip cef accounting per-prefix` | Enables Cisco Express Forwarding network accounting.<br>• The **non-recursive** keyword enables you to count the number of packets and bytes express forwarded through nonrecursive prefixes.<br>This keyword is optional when the command is used in global configuration mode.<br>• The **per-prefix** keyword enables you to count the number of packets and bytes express forwarded to a destination IP address (or prefix).<br>• The **prefix-length** keyword enables accounting based on prefix length. |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits to privileged EXEC mode. |

# Enabling a Backbone Router to Collect TMS

This section contains information about and instructions for enabling a backbone router to collect TMS for Cisco Express Forwarding. Enabling a backbone router to collect TMS requires enabling nonrecursive accounting and setting the interfaces on the router to collect internal or external TMS. The internal and external settings are used only for TMS collection. The interfaces are set to internal by default.

**Note** Make sure you configure the collection of internal and external TMS on the incoming interface of the backbone router.

You can perform these tasks either through the CLI or through the NDA. The following sections explain each procedure:

## Using the CLI to Enable a Backbone Router to Collect TMS

Perform the following task to use the CLI to enable a backbone router to collect TMS.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **ip cef accounting** {[**non-recursive** [**per-prefix**] [**prefix-length**]}
5. **interface** *type slot* / *subslot* / *port* [.*subinterface-number*]
6. **ip cef accounting non-recursive**
7. **exit**

8. Repeat Steps 5, 6, and 7 for each incoming interface that you want to configure for TMS.
9. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip cef**<br>**Example:**<br>`Router(config)# ip cef` | Enables Cisco Express Forwarding on the route processor card. |
| **Step 4** | **ip cef accounting** {[**non-recursive** [**per-prefix**] [**prefix-length**]}<br>**Example:**<br>`Router(config)# ip cef accounting non-recursive` | Enables Cisco Express Forwarding network accounting.<br>• The **non-recursive** keyword enables you to count the number of packets and bytes express forwarded through nonrecursive prefixes.<br>This keyword is optional when the command is used in global configuration mode.<br>• The **per-prefix** keyword enables you to count the number of packets and bytes express forwarded to a destination (or prefix).<br>• The **prefix-length**keyword enables accounting based on prefix length. |
| **Step 5** | **interface** *type slot* / *subslot* / *port* [.*subinterface-number*]<br>**Example:**<br>`Router(config)# interface fastethernet 1/1/0`<br>**Example:** | Configures an interface type and enters interface configuration mode.<br>• The *type* argument is the type of interface to be configured.<br>• The *slot* argument is the chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. |

| | Command or Action | Purpose |
|---|---|---|
| | | - The / *subslot* keyword and argument pair is the secondary slot number on a SIP where a SPA is installed. The slash (/) is required.<br>Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.<br>- The / *port* keyword and argument pair is the port or interface number. The slash (/) is required.<br>Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide<br>- The **.** *subinterface-number*keyword and argument pair is the subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs.<br>This command specifies the interface on the backbone router that you intend to configure. |
| **Step 6** | **ip cef accounting non-recursive**<br>**Example:**<br>`Router(config-if)# ip cef accounting non-recursive` | Enables nonrecursive accounting on the router. |
| **Step 7** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits to global configuration mode. |
| **Step 8** | Repeat Steps 5, 6, and 7 for each incoming interface that you want to configure for TMS. | -- |
| **Step 9** | **end**<br>**Example:**<br>`Router(config-if)# end` | Exits to privileged EXEC mode. |

## Enabling the NDA to Collect TMS on a Backbone Router

Perform the following task to enable the NDA to collect TMS on a backbone router.

You can use the NDA to enable TMS collection and to set the incoming interfaces on the backbone router to collect internal or external traffic data.

## SUMMARY STEPS

1. Open the Traffic Matrix Statistics Control window in the NDA.
2. Click the **New** button in the Traffic Matrix Statistics Control window.
3. Specify the new TMS collection parameters, using the Traffic Matrix Statistics Control window.
4. Click **OK** in the New Collection panel.
5. Select the **TMS** tab in the Router Configuration window in the NDA.
6. Set internal and external interfaces on the router.
7. Click **Apply**in the Router Configuration window.

## DETAILED STEPS

**Step 1** Open the Traffic Matrix Statistics Control window in the NDA.

For specific instructions, refer to the Network Data Analyzer Installation and User Guide.

**Step 2** Click the **New** button in the Traffic Matrix Statistics Control window.

If a valid directory of router configuration files exists on a designated UtilityServer host in the network, the Traffic Matrix Statistics Control window shown in the first figure below appears.

**Step 3** Specify the new TMS collection parameters, using the Traffic Matrix Statistics Control window.

The window incorporates a New Collection panel that enables you to define a new TMS collection process. To use the NDA for TMS collection, you must specify the following information:

- The name of the collection (Collection ID)--Enter an alphanumeric name of any length without embedded spaces for the TMS collection process on the selected router (see next bullet).
- The router from which you want to collect TMS--Use the drop-down box to choose the name of a network device where you want to collect TMS.
- How often and how long to collect TMS--Specify each of the following in minutes:
  - How much time is to elapse before the TMS collection process begins ("Start in" field)
  - The overall duration of the TMS collection process ("collect for" field)
  - How often "snapshots" of the traffic counters in the selected router are to be exported to the designated TMS data repository ("every" field)

The window for entering this information on the NDA is similar to the one shown in the figure below.

**Step 4** Click **OK** in the New Collection panel.

The Traffic Matrix Statistics Control window confirms the information you entered, and the new collection name appears at the top left corner of the window.

**Step 5** Select the **TMS** tab in the Router Configuration window in the NDA.

The TMS Router Configuration panel shown in the figure below appears. This panel enables you to configure network devices to export TMS data. (For instructions on locating the Router Configuration window, refer to the Network Data Analyzer Installation and User Guide .)

**Step 6** Set internal and external interfaces on the router.

The Router Configuration window allows you to set the interfaces on the backbone router to collect internal and external packet and byte data. By default, all interfaces are set to collect internal data. Single-selection buttons allow you to associate the interface with either internal data or external data. You can select only one radio button for an interface at one time. Set the interface to collect internal or external data by clicking the appropriate radio button.

The window for selecting this information on the NDA is similar to the one shown in the figure below.

**Step 7** Click **Apply**in the Router Configuration window.

Any changes that you have made to the configuration parameters in the TMS Router Configuration panel are applied to the currently selected device. The Apply button affects only changes made in the panel where the button is located. When the NDA asks if you want to enable Cisco Express Forwarding, click **Yes**.

# Interpreting the tmstats File

This section contains instructions for interpreting the statistics in the tmstats_ascii file. For conceptual information about the tmstats_ascii file, see the Statistics in the timestats File, on page 95.

### SUMMARY STEPS

1. **more system:/vfiles/tmstats_ascii**
2. Interpret the header and record information in the tmstats_ascii file.

### DETAILED STEPS

**Step 1** **more system:/vfiles/tmstats_ascii**

Enter this command on the backbone router to view the statistics in the ASCII file. For example:

**Example:**

```
Router# more system:/vfiles/tmstats_ascii
VERSION 1|ADDR 172.27.32.24|AGGREGATION TrafficMatrix.ascii|SYSUPTIME 41428|routerUTC 3104467160|NTP
 unsynchronized|DURATION 1|
p|10.1.0.0/16|242|1|50|2|100
p|172.27.32.0/22|242|0|0|0|0
```

This is an example of a tmstats_ascii file. The example contains a header information and two records. The header information and each record begin on a separate line. A bar (|) separates consecutive fields within a header or record. The first field in a record specifies the type of record.

**Step 2** Interpret the header and record information in the tmstats_ascii file.

Each tmstats_ascii file displayed consists of header information and records. The file in the example in Step 1 contains header information and two destination prefix records.

Refer to the following sections for a description of header and record information:

# Viewing Information in the tmsasinfo File

Perform the following task to view information in the tmsasinfo file about BGP neighbor autonomous systems (ASs) for IGP destinations.

The TMS feature also displays the BGP neighbor ASs associated with each IGP destination. You can display all the neighbor ASs for any IGP destination. The tmsasinfo file is in ASCII format. It is the only format provided for this data.

For conceptual information about the tmsasinfofile, see the Statistics in the tmsasinfo File, on page 98.

### SUMMARY STEPS

1. **more system:/vfiles/tmsasinfo**
2. View the header and record information in the tmasinfo file.

### DETAILED STEPS

**Step 1** **more system:/vfiles/tmsasinfo**

Enter this command on the backbone router to view the statistics in the tmsasinfo ASCII file. For example:

**Example:**

```
Router# more system:/vfiles/tmsasinfo

VERSION 1|ADDR 10.10.10.10|AGGREGATION ASList.ascii|SYSUPTIME 619855|routerUTC 3334075555|DURATION
0
10.1.1.2/32|65535|192.168.1.0/24
This is an example of a tmsasinfo file. The example contains a header information and one record.
The header information and each record begin on a separate line. A bar (|) separates consecutive
fields within a header or record.
```

**Step 2** View the header and record information in the tmasinfo file.

Refer to the following sections for a description of header and record information:

# Verifying CEF Network Accounting Information

Perform the following task to verify that Cisco Express Forwarding networking accounting information is as you expected.

### SUMMARY STEPS

1. **enable**
2. **show ip cef summary**
3. **show ip cef** *interface* **-** *type slot* / *subslot* / *port* [**.** *subinterface-number*] **detail**
4. **disable**

## DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip cef summary**

Use this command to display the collected Cisco Express Forwarding network accounting information. For example:

**Example:**

```
Router# show ip cef summary
IP CEF with switching (Table Version 19), flags=0x0
  19 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 1
  19 leaves, 17 nodes, 19960 bytes, 58 inserts, 39 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id E3296D5B
  3(1) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts:  4628 leaf, 4608 node
Adjacency Table has 7 adjacencies
```

This command shows sample accounting information on a router with Central Cisco Express Forwarding enabled. In this example, the Cisco Express Forwarding table contains a total or 19 entries, 0 entries need to be reresolved, 0 entries do not have resolved recursions, and the highest number of unresolved entries is 1. The Cisco Express Forwarding Trie contains 19 leaves and 17 nodes, which take up 19960 bytes of memory. The number of routes inserted into the table is 58 and 39 routes have been invalidated. This command shows no load sharing elements. The per-destination load sharing algorithm is configured and the identifier is E3296D5D.

**Example:**

The following command is sample output for a router with distributed Cisco Express Forwarding enabled:

**Example:**

```
Router# show ip cef summary
IP Distributed CEF with switching (Table Version 36), flags=0x0
  16 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 1
  19 leaves, 17 nodes, 19960 bytes, 39 inserts, 20 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id E3296D5B
  2(0) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts:  4628 leaf, 4608 node
```

**Step 3** **show ip cef** *interface* **-** *type slot* **/** *subslot* **/** *port* [**.** *subinterface-number*] **detail**

Use this command to show detailed Cisco Express Forwarding network accounting information for a specified interface type and number. The following is sample output from the **show ip cef detail**command for interface FastEthernet 0/0/0.

It shows all the prefixes resolving through adjacency pointing to next hop interface FastEthernet 0/0/0 and next hop interface IP address 172.29.233.33.

For example, for FastEthernet interface 0/0/0, IP address 172.29.233.33:

**Example:**

```
Router# show ip cef fastethernet 0/0/0 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
 172.29.233.33/32, version 7417, cached adjacency 172.29.233.33
 0 packets, 0 bytes,
   Adjacency-prefix
   via 172.29.233.33, FastEthernet0/0/0, 0 dependencies
 next hop 172.29.233.33, FastEthernet0/0/0
   valid cached adjacency
 0 packets, 0 bytes switched through the prefix
 tmstats: external 0 packets, 0 bytes
      internal 0 packets, 0 bytes
```

**Step 4** **disable**

Use this command to exit to user EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

# Configuration Examples for CEF Network Accounting

## Example Configuring CEF Network Accounting

The following example shows how to enable the collection of Cisco Express Forwarding accounting information:

```
configure terminal
!
ip cef accounting
end
```

## Example Enabling a Backbone Router to Collect TMS Data

The following example shows how to enable a backbone router to collect TMS data:

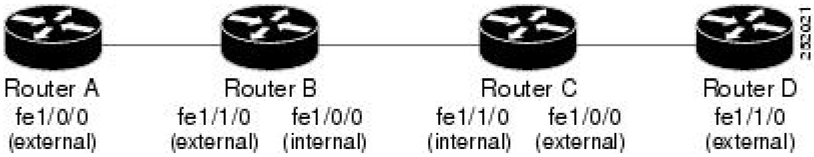
```
configure terminal
!
ip cef
ip cef accounting non-recursive
!
interface fe1/0/0
 ip cef accounting non-recursive external
 end
```

For a sample backbone configuration, see the Example IP CEF Nonrecursive Accounting, on page 108 section.

# Example IP CEF Nonrecursive Accounting

The following example shows an IP Cisco Express Forwarding accounting configuration. The example shows how to enable routers to count the number of internal and external packets and bytes that travel through the backbone routers. The figure below shows the sample backbone configuration.

*Figure 5: Sample Backbone Configuration*



### Router A Configuration

```
Router(config)# ip cef
Router(config)# ip cef accounting non-recursive
Router(config)# interface fe1/0/0
Router(config-if)# ip cef accounting non-recursive external
```

### Router B Configuration: fe1/1/0

```
Router(config)# ip cef
Router(config)# ip cef accounting non-recursive
Router(config)# interface fe1/1/0

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

### Router B Configuration: fe1/0/0:

```
Router(config)# interface fe1/0/0
Router(config-if)# ip cef accounting non-recursive internal
```

### Router C Configuration: fe1/1/0:

```
Router(config)# ip cef
Router(config)# ip cef accounting non-recursive
Router(config)# interface fe1/1/0

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

### Router C Configuration: fe1/0/0:

```
Router(config)# interface fe1/0/0
Router(config-if)# ip cef accounting non-recursive external
```

### Router D Configuration

```
Router(config)# ip cef
Router(config)# ip cef accounting non-recursive
Router(config)# interface fe1/1/0

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

## Example Interpreting the tmstats_ascii File

The following example shows the contents of tmstats_ascii file:

```
Router# more system:/vfiles/tmstats_ascii
VERSION 1|ADDR 172.27.32.24|AGGREGATION TrafficMatrix.ascii|SYSUPTIME 41428|routerUTC
3104467160|NTP unsynchronized|DURATION 1|
p|10.1.0.0/16|242|1|50|2|100
p|172.27.32.0/22|242|0|0|0|0
```

This example contains header information and two destination prefix records. The records represent dynamic label switching or traffic engineering (TE) tunnel data indicated by the initial "p."

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Overview of the Cisco Express Forwarding feature | Cisco Express Forwarding Overview |
| Tasks for enabling or disabling Cisco Express Forwarding or distributed Cisco Express Forwarding | Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding to Customize Switching and Forwarding for Dynamic Networks |
| Tasks for configuring load-balancing schemes for Cisco Express Forwarding | Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic |
| Tasks for configuring Cisco Express Forwarding consistency checkers | Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards |
| Tasks for configuring epochs for Cisco Express Forwarding tables | Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables |

| Related Topic | Document Title |
|---|---|
| Commands for configuring and managing Cisco Express Forwarding | *Cisco IOS IP Switching Command Reference* |
| Tasks for customizing the display of Cisco Express Forwarding event trace messages | Customizing the Display of Cisco Express Forwarding Event Trace Messages |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | -- |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for CEF Network Accounting

*Table 16: Feature Information for Configuring Cisco Express Forwarding Network Accounting*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| This table is intentionally left blank because no features were introduced or modified in Cisco IOS XE Release 2.1 or later. | -- | -- |

# Glossary

**adjacency** --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

**Cisco Express Forwarding** --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

**distributed Cisco Express Forwarding** --A mode of Cisco Express Forwarding operation in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

**FIB** --forwarding information base. A component of Cisco Express Forwarding that is conceptually similar to a routing table or information base. The router uses the FIB lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

**GRE** --generic routing encapsulation. A tunneling protocol developed by Cisco that enables encapsulation of a wide variety of protocol packet types inside IP tunnels. GRE creates a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows the expansion of a network across a single-protocol backbone environment.

**IPC** --interprocess communication. The mechanism that enables the distribution of Cisco Express Forwarding tables from the Route Switch Processor (RSP) to the line card when the router is operating in distributed Cisco Express Forwarding mode.

**label disposition** --The removal of Multiprotocol Label Switching (MPLS) headers at the edge of a network. In MPLS label disposition, packets arrive on a router as MPLS packets and, with the header removed, are transmitted as IP packets.

**label imposition** --The action of putting a label on a packet.

**LER** --label edge router. A router that performs label imposition.

**LFIB** --Label Forwarding Information Base. The data structure used by switching functions to switch labeled packets.

**LIB** --Label information base. A database used by a label switch router (LSR) to store labels learned from other LSRs, as well as labels assigned by the local LSR.

**line card** --A general term for an interface processor that can be used in various Cisco products. For example, a Versatile Interface Processor (VIP) is a line card for the Cisco 7500 series router.

**LSP** --label switched path. A sequence of hops (Router 0...Router n). A packet travels from R0 to Rn by means of label switching mechanisms. An LSP can be chosen dynamically, based on normal routing mechanisms, or you can configure the LSP manually.

**LSR** --label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MPLS** --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along the normal routing paths (sometimes called MPLS hop-by-hop forwarding).

**prefix** --The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are the network bits. For example, 1.0.0.0/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 10.0.

**RIB** --Routing Information Base. A central repository of routes that contains Layer 3 reachability information and destination IP addresses or prefixes. The RIB is also known as the routing table.

**RP** --Route Processor. The processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a supervisory processor.

**RSP** --Route Switch Processor. The processor module used in the Cisco 7500 series routers that integrates the functions of the Route Processor (RP) and the Switch Processor (SP).

**SP** --Switch Processor. Cisco 7000-series processor module that acts as the administrator for all CxBus activities. It is also sometimes called a CiscoBus controller.

**VIP** --Versatile Interface Processor. An interface card used in Cisco 7000 and Cisco 7500 series routers. The VIP provides multilayer switching and runs Cisco IOS software.

**VPN** --Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** --A Virtual Private Network (VPN) routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

CHAPTER 10

# Customizing the Display of CEF Event Trace Messages

This module contains information about and instructions for customizing the display of recorded Cisco Express Forwarding events.

You can customize the Cisco Express Forwarding event-tracing message display by specifying the size of the file stored in memory or by choosing to display event trace messages by prefix and mask, by a specified interface, or by a Cisco Express Forwarding Virtual Private Network (VPN) routing and forwarding instance (VRF) for an IPv4 or IPv6 address family.

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

# Prerequisites for the Display of CEF Event Trace Messages

Cisco Express Forwarding must be running on the networking device before you can customize the display of recorded Cisco Express Forwarding events.

# Restrictions for the Display of CEF Event Trace Messages

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 process switched. Logging disables Cisco Express Forwarding.

# Information About the Display of CEF Event Trace Messages

## Cisco Platform Support for Central CEF and dCEF

Cisco Express Forwarding is enable by default on the Cisco ASR 1000 Series Aggregation Services Routers.

To find out if Cisco Express Forwarding is enabled on your platform, enter the **show ip cef**command. If Cisco Express Forwarding is enabled, you receive output that looks like this:

```
Router# show ip cef
Prefix              Next Hop            Interface
[...]
10.2.61.8/24        192.168.100.1       FastEthernet1/0/0
                    192.168.101.1       FastEthernet2/1/0
[...]
```

If Cisco Express Forwarding is not enabled on your platform, the output for the **show ip cef**command looks like this:

```
Router# show ip cef
%CEF not running
```

If Cisco Express Forwarding is not enabled on your platform, use the **ip cef**command to enable (central) Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

## Overview of CEF Event Trace Function

The Cisco Express Forwarding event trace function collects Cisco Express Forwarding events as they occur, even when debugging is not enabled. This function allows the tracing of an event immediately after it occurs. Cisco technical personnel can use the event trace function to help resolve any problems with the Cisco Express Forwarding feature.

Cisco Express Forwarding event trace messages are saved in memory on the device. When the event trace messages exceed the configured size, the newest message in the trace will begin to overwrite the older messages. You can use the following commands to change the capacity of the Cisco Express Forwarding event message file:

- The **monitor event-trace cef events size**global configuration command allows you to increase or decrease the number of messages that can be written to memory for a single instance of a trace. To display the size parameter, use the **show monitor event-trace events parameters** command.
- The **monitor event-trace cef events clear** privileged EXEC command allows you to clear existing trace messages.
- The **monitor event-trace cef**(global) command configures event tracing for Cisco Express Forwarding events. To monitor and control the event trace function for Cisco Express Forwarding events, use the **monitor event-trace cef** (EXEC) command.

You can use the following commands to display Cisco Express Forwarding events:

- The **show monitor event-trace cef all**command displays all event trace messages currently in memory for Cisco Express Forwarding.
- The **debug ip cef** command and the **events** keyword record general Cisco Express Forwarding events as they occur.
- The **debug ip cef table**command enables the real-time collection of events that affect entries in the Cisco Express Forwarding tables.

# CEF Event Tracing Defaults and Options

Event tracing for distributed Cisco Express Forwarding events is enabled by default. The Cisco IOS XE 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.

To configure the file in which you want to save trace information, use the **monitor event-trace cef**command in global configuration mode. By default, the trace messages are saved in a 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 in privileged EXEC mode. The amount of data collected from a 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.

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

## CEF Event Tracing for IPv4 Events

Event tracing for Cisco Express Forwarding IPv4 events is enabled by default. The 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.

To configure the file in which you want to save trace information for Cisco Express Forwarding IPv4 events, use the **monitor event-trace cef ipv4**command in global configuration mode. By default, the trace messages are saved in a binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace cef ipv4 dump pretty** command in privileged EXEC mode. 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.

## CEF Event Tracing for IPv6 Events

Event tracing for Cisco Express Forwarding IPv6 events is enabled by default.The Cisco IOS XE 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.

To configure the file in which you want to save trace information for Cisco Express Forwarding IPv6 events, use the **monitor event-trace cef ipv6**command in global configuration mode. By default, the trace messages are saved in a binary format. If you want to save trace messages in ASCII format, possibly for additional application processing, use the **monitor event-trace cef ipv6 dump pretty** command in privileged EXEC mode. 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, 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.

# How to Customize the Display of CEF Event Trace Messages

Perform the following tasks to customize the Cisco Express Forwarding event tracing function and to display event trace messages:

## Customizing CEF Event Tracing

Perform the following task to customize Cisco Express Forwarding event tracing. Event trace messages can be used to monitor Cisco Express Forwarding and to help resolve any issues with the Cisco Express Forwarding feature.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace cef** {**dump-file** *dump-file-name* | {**events** | **interface**} {**disable** | **dump-file** *dump-file-name*| **enable** | **size** *number* | **stacktrace** [*depth*]}}
4. **exit**
5. **monitor event-trace cef** {**dump** [**merged pretty** | **pretty**] | {**events** | **interface** | **ipv4** | **ipv6**} {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}}
6. **disable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **monitor event-trace cef** {**dump-file** *dump-file-name* \| {**events** \| **interface**} {**disable** \| **dump-file** *dump-file-name*\| **enable** \| **size** *number* \| **stacktrace** [*depth*]}}<br>**Example:**<br>`Router(config)# monitor event-trace cef dump-file tftp://172.16.10.5/cef-events` | Configures event tracing for Cisco Express Forwarding.<br>• The **dump-file** *dump-file-name* keyword and argument pair specify 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.<br>• The **events**keyword turns on event tracing for Cisco Express Forwarding events.<br>• The **interface** keyword turns on event tracing for Cisco Express Forwarding interface events.<br>• The **disable** keyword turns off event tracing for Cisco Express Forwarding events.<br>• The **enable** keyword turns on event tracing for Cisco Express Forwarding events if it had been enabled with the **monitor event-trace cef** privileged EXEC command.<br>• The **size** *number* keyword and argument pair sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536.<br>**Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef events parameters** command.<br>• The **stacktrace** keyword enables the stack trace at tracepoints.<br>• The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits to privileged EXEC mode. |
| **Step 5** | **monitor event-trace cef** {**dump** [**merged pretty** \| **pretty**] \| {**events** \| **interface** \| **ipv4** \| **ipv6**} {**clear** \| **continuous** [**cancel**] \| **disable** \| **dump** [**pretty**] \| **enable** \| **one-shot**}}<br>**Example:**<br>`Router# monitor event-trace cef events dump pretty` | Monitors and controls the event trace function for Cisco Express Forwarding.<br>• The **dump** keyword writes the event trace results to the file configured with the **monitor event-trace cef**global configuration command. The trace messages are saved in binary format.<br>• The **merged pretty** keywords sort all event trace entries by time and write the entries to a file in ASCII format.<br>• The **pretty** keyword saves the event trace message in ASCII format.<br>• The **events** keyword monitors Cisco Express Forwarding events.<br>• The **interface**keyword monitors Cisco Express Forwarding interface events.<br>• The **ipv4**keyword monitors Cisco Express Forwarding IPv4 events.<br>• The **ipv6** keyword monitors Cisco Express Forwarding IPv6 events.<br>• The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device.<br>• The **continuous** keyword continuously displays the latest event trace entries.<br>• The **cancel** keyword cancels the continuous display of the latest trace entries.<br>• The **disable** keyword turns off Cisco Express Forwarding event tracing.<br>• The **enable** keyword turns on Cisco Express Forwarding event tracing.<br>• The **one-shot** keyword 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 or Action | Purpose |
|---|---|---|
| **Step 6** | **disable**<br>**Example:**<br>`Router# disable` | Exits to user EXEC mode. |

# Customizing CEF Event Tracing for IPv4 Events

Perform the following task to customize Cisco Express Forwarding event tracing for Cisco Express Forwarding IPv4 events. Use event tracing to monitor Cisco Express Forwarding IPv4 events as they occur and to help resolve any issues with Cisco Express Forwarding and related IPv4 events.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **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*}]}
4. **exit**
5. **monitor event-trace cef ipv4** {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}
6. **disable**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **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*}]}<br>**Example:**<br>`Router(config)# monitor event-trace cef ipv4 size 10000` | Configures event-tracing for Cisco Express Forwarding IPv4 events.<br>• The **disable** keyword turns off event tracing for Cisco Express Forwarding IPv4 events.<br>• The **distribution** keyword logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards<br>• The **dump-file** *dump-file-name* keyword and argument pair specify the file to which event trace messages are written from memory on the networking device. The |

| | Command or Action | Purpose |
|---|---|---|
| | | 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.<br>• The **enable** keyword turns on event tracing for Cisco Express Forwarding IPv4 events if it had been enabled with the **monitor event-trace cef** privileged EXEC command.<br>• The **match**keyword turns on event tracing for Cisco Express Forwarding IPv4 events that matches global events or events that match a specific network address<br>• The **global**keyword specifies global events.<br>• The *ip-address mask*argumentsspecify an IP address in A.B.C.D format and a subnet mask in A.B.C.D format.<br>• The **size** *number* keyword and argument pair sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536.<br>**Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef ipv4 parameters** command.<br>• The **stacktrace** keyword enables the stack trace at tracepoints.<br>• The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16.<br>• The **vrf** *vrf-name* keyword and argument pair turns on event tracing for a Cisco Express Forwarding IPv4 VRF table. The *vrf-name* argument specifies the name of the VRF |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits to privileged EXEC mode. |
| **Step 5** | **monitor event-trace cef ipv4** {**clear** \| **continuous** [**cancel**] \| **disable** \| **dump** [**pretty**] \| **enable** \| **one-shot**}<br>**Example:**<br>`Router# monitor event-trace cef ipv4 continuous` | Monitors and controls the event trace function for Cisco Express Forwarding IPv4 events.<br>• The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device. |

| | Command or Action | Purpose |
|---|---|---|
| | | • The **continuous** keyword continuously displays the latest event trace entries.<br>• The **cancel** keyword cancels the continuous display of the latest trace entries.<br>• The **disable** keyword turns off Cisco Express Forwarding event tracing.<br>• The **dump** keyword 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.<br>• The **pretty** keyword saves the event trace message in ASCII format.<br>• The **enable** keyword turns on Cisco Express Forwarding event tracing.<br>• The **one-shot** keyword 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. |
| **Step 6** | **disable**<br>**Example:**<br>`Router# disable` | Exits to user EXEC mode. |

# Customizing CEF Event Tracing for IPv6 Events

Perform the following task to customize Cisco Express Forwarding event tracing for Cisco Express Forwarding IPv6 events.Use event tracing to monitor Cisco Express Forwarding IPv6 events as they occur and to help resolve any issues with Cisco Express Forwarding and related IPv6 events.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace cef ipv4** {**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}*]}
4. **exit**
5. **monitor event-trace cef ipv6** {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}}
6. **disable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **monitor event-trace cef ipv4** {**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}*]}<br>**Example:**<br>`Router(config)# monitor event-trace cef ipv6 match global` | Configures event-tracing for Cisco Express Forwarding IPv6 events.<br>• The **disable** keyword turns off event tracing for Cisco Express Forwarding IPv6 events.<br>• The **distribution** keyword logs events related to the distribution of Cisco Express Forwarding FIB tables to the line cards.<br>• The **dump-file** *dump-file-name* keyword and argument pair specify 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.<br>• The **enable** keyword turns on event tracing for Cisco Express Forwarding IPv6 events if it had been enabled with the **monitor event-trace cef** privileged EXEC command.<br>• The **match**keyword turns on event tracing for Cisco Express Forwarding IPv6 events that matches global events or events that match a specific network address.<br>• The **global**keyword specifies global events.<br>• The *ipv6-address* / *n*argument 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 (/ *n*) indicates the number of bits that do not change. Range: 0 to 128<br>• The **size** *number* keyword and argument pair sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef ipv6 parameters** command.<br>• The **stacktrace** keyword enables the stack trace at tracepoints.<br>• The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16.<br>• The **vrf** *vrf-name* keyword and argument pair turns on event tracing for a Cisco Express Forwarding IPv6 VRF table. The *vrf-name* argument specifies the name of the VRF |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits to privileged EXEC mode. |
| **Step 5** | **monitor event-trace cef ipv6** {**clear** \| **continuous** [**cancel**] \| **disable** \| **dump** [**pretty**] \| **enable** \| **one-shot**}}<br>**Example:**<br>`Router# monitor event-trace cef ipv6 one-shot` | Monitors and controls the event trace function for Cisco Express Forwarding IPv6 events.<br>• The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device.<br>• The **continuous** keyword continuously displays the latest event trace entries.<br>• The **cancel** keyword cancels the continuous display of the latest trace entries.<br>• The **disable** keyword turns off Cisco Express Forwarding event tracing.<br>• The **dump** keyword 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.<br>• The **pretty** keyword saves the event trace message in ASCII format.<br>• The **enable** keyword turns on Cisco Express Forwarding event tracing.<br>• The **one-shot** keyword 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 or Action | Purpose |
|---|---|---|
| **Step 6** | **disable**<br>**Example:**<br>`Router# disable` | Exits to privileged EXEC mode. |

# Displaying CEF Event Trace Information

Perform the following task to display Cisco Express Forwarding event trace information.

## SUMMARY STEPS

1. **enable**
2. **monitor event-trace cef events clear**
3. **debug ip cef table**
4. **show monitor events-trace cef all**
5. **show monitor event-trace cef latest**
6. **show monitor event-trace cef events all**
7. **show monitor event-trace cef interface latest**
8. **show monitor event-trace cef ipv4 all**
9. **show monitor event-trace cef ipv6 parameters**
10. **disable**

## DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **monitor event-trace cef events clear**

Use this command to clear the Cisco Express Forwarding event trace buffer. For example:

```
Router# monitor event-trace cef clear
```

**Example:**

**Step 3** **debug ip cef table**

Use this command to display events that affect entries in the Cisco Express Forwarding tables. For example:

**Example:**

```
Router# debug ip cef table
```

```
01:25:46:CEF-Table:Event up, 10.1.1.1/32 (rdbs:1, flags:1000000)
01:25:46:CEF-IP:Checking dependencies of 0.0.0.0/0
01:25:47:CEF-Table:attempting to resolve 10.1.1.1/32
01:25:47:CEF-IP:resolved 10.1.1.1/32 via 10.9.104.1 to 10.9.104.1 Ethernet2/0/0
01:26:02:CEF-Table:Event up, default, 0.0.0.0/0 (rdbs:1, flags:400001)
01:26:02:CEF-IP:Prefix exists - no-op change
```

**Step 4** **show monitor events-trace cef all**

Use this command to display event trace messages for Cisco Express Forwarding. For example:

**Example:**

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

cef_interface:
*Jul 22 20:14:58.999: Et0/0        (hw  3) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/1        (hw  4) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/2        (hw  5) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/3        (hw  6) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et1/0        (hw  7) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et1/1        (hw  8) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et1/2        (hw  9) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et1/3        (hw 10) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Se2/0        (hw 11) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Se2/1        (hw 12) SWvecLES <unknown> (0x01096A3C)
.
.
.
```

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

**Step 5** **show monitor event-trace cef   latest**

Use this command to display only the event trace message that have been sent since the last instance of the **show monitor event-trace cef** command. For example:

**Example:**

```
Router# show monitor event-trace cef latest
cef_events:
```

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

**Step 6** **show monitor event-trace cef   events   all**

Use this command to display information about Cisco Express Forwarding events. For example:

**Example:**

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

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

For example, the Subsys event type is related to the initialization of a subset of Cisco Express Forwarding functionality. The "ipv4fib_ios_def_cap init" entry is the initialization of IPv4 Cisco Express Forwarding default capabilities.

**Step 7** **show monitor event-trace cef   interface latest**

Use this command to display only the event trace messages generated since the last **show monitor event-trace cef interface**command was entered. For example:

**Example:**

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

```
*Jul 22 20:14:58.999: Et0/0        (hw  3) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/1        (hw  4) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/2        (hw  5) SWvecLES <unknown> (0x01096A3C)
*Jul 22 20:14:58.999: Et0/3        (hw  6) SWvecLES <unknown> (0x01096A3C)
.
.
.
*Jul 22 20:14:59.075: <empty>      (hw  3) State    down -> up
*Jul 22 20:14:59.075: <empty>      (hw  3) Create   new
*Jul 22 20:14:59.075: Et0/0        (hw  3) NameSet
*Jul 22 20:14:59.075: Et0/0        (hw  3) HWIDBLnk Ethernet0/0(3)
*Jul 22 20:14:59.075: Et0/0        (hw  3) RCFlags  None -> Fast
*Jul 22 20:14:59.075: <empty>      (sw  3) VRFLink  IPv4:id0 - success
*Jul 22 20:14:59.075: <empty>      (sw  3) State    deleted -> down
*Jul 22 20:14:59.075: <empty>      (sw  3) Create   new
*Jul 22 20:14:59.075: Et0/0        (sw  3) NameSet
*Jul 22 20:14:59.075: Et0/0        (sw  3) FIBHWLnk Ethernet0/0(3)
*Jul 22 20:14:59.075: Et0/0        (sw  3) SWIDBLnk Ethernet0/0(3)
*Jul 22 20:14:59.075: Et0/0        (sw  3) FlagCha  0x6000 add input|first
*Jul 22 20:14:59.075: Et0/0        (sw  3) State    down -> up
*Jul 22 20:14:59.075: <empty>      (hw  4) State    down -> up
*Jul 22 20:14:59.075: <empty>      (hw  4) Create   new
*Jul 22 20:14:59.075: Et0/1        (hw  4) NameSet
*Jul 22 20:14:59.075: Et0/1        (hw  4) HWIDBLnk Ethernet0/1(4)
*Jul 22 20:14:59.075: Et0/1        (hw  4) RCFlags  None -> Fast
*Jul 22 20:14:59.075: <empty>      (sw  4) VRFLink  IPv4:id0 - success
*Jul 22 20:14:59.075: <empty>      (sw  4) State    deleted -> down
*Jul 22 20:14:59.075: <empty>      (sw  4) Create   new
*Jul 22 20:14:59.075: Et0/1        (sw  4) NameSet
*Jul 22 20:14:59.075: Et0/1        (sw  4) FIBHWLnk Ethernet0/1(4)
*Jul 22 20:14:59.075: Et0/1        (sw  4) SWIDBLnk Ethernet0/1(4)
*Jul 22 20:14:59.075: Et0/1        (sw  4) FlagCha  0x6000 add input|first
*Jul 22 20:14:59.075: Et0/1        (sw  4) State    down -> up
.
.
.
```

**Step 8** **show monitor event-trace cef ipv4 all**

Use this command to display information about Cisco Express Forwarding IPv4 events. For example:

**Example:**

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

**Step 9** **show monitor event-trace cef ipv6 parameters**

Use this commands to display parameters configured for Cisco Express Forwarding IPv6 events. For example:

**Example:**

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

**Step 10** **disable**

Use this command to exit to user EXEC mode. For example:

**Example:**

```
Router# disable
Router>
```

# Configuration Examples for the Display of CEF Event Trace Messages

## Customizing CEF Event Tracing Examples

The following example shows how to enable event tracing for Cisco Express Forwarding and configure the buffer size to 2500 messages. The trace messages file is set to cef-dump in slot0 (flash memory).

```
configure terminal
!
monitor event-trace cef events enable
monitor event-trace cef dump-file slot0:cef-dump
monitor event-trace cef events size 2500
exit
The following example shows what happens when you try to enable event tracing for Cisco
Express Forwarding events when it is already enabled:
configure terminal
!
monitor event-trace cef events enable
00:04:33: %EVENT_TRACE-6-ENABLE: Trace already enabled.
```

The following example shows the privileged EXEC commands that stop event tracing, clear the current contents of memory, and reenable the trace function for Cisco Express Forwarding events. This example assumes that the tracing function is configured and enabled on the networking device.

```
enable
!
monitor event-trace cef events disable
monitor event-trace cef events clear
monitor event-trace cef events enable
disable
```

## Example Customizing CEF Event Tracing for IPv4 Events

The following example shows how to enable event tracing for Cisco Express Forwarding IPv4 events and configure the buffer size to 5000 messages:

```
configure terminal
!
monitor event-trace cef ipv4 enable
monitor event-trace cef ipv4 size 5000
exit
The following example shows how to enable event tracing for events that match Cisco Express
 Forwarding IPv4 VRF vpn1:
configure terminal
!
monitor event-trace cef ipv4 enable
monitor event-trace cef ipv4 vrf vpn1
exit
```

The following example shows the privileged EXEC commands to configure the continuous display of the latest Cisco Express Forwarding event trace entries for IPv4 events:

```
enable
!
monitor event-trace cef ipv4 continuous
disable
```

The following example shows how to stop the continuous display of the latest trace entries:

```
enable
!
monitor event-trace cef ipv4 continuous cancel
disable
```

## Example Customizing CEF Event Tracing for IPv6 Events

The following example shows how to enable event tracing for Cisco Express Forwarding IPv6 events and configure the buffer size to 10000:

```
configure terminal
!
monitor event-trace cef ipv6 enable
monitor event-trace cef ipv6 size 10000
exit
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Commands for configuring and managing Cisco Express Forwarding | *Cisco IOS IP Switching Command Reference* |
| Overview of the Cisco Express Forwarding feature | Cisco Express Forwarding Overview |

| Related Topic | Document Title |
|---|---|
| Tasks for verifying basic Cisco Express Forwarding and distributed Cisco Express Forwarding operation | Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks |
| Tasks for enabling or disabling Cisco Express Forwarding or distributed Cisco Express Forwarding | Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding to Customize Switching and Forwarding for Dynamic Networks |
| Tasks for configuring load-balancing schemes for Cisco Express Forwarding | Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic |
| Tasks for configuring Cisco Express Forwarding consistency checkers | Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards |
| Tasks for configuring epochs for Cisco Express Forwarding tables | Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables |
| Tasks for configuring and verifying Cisco Express Forwarding network accounting | Configuring Cisco Express Forwarding Network Accounting |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | -- |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for the Display of CEF Event Trace Messages

*Table 17: Feature Information for Configuring the Display of Cisco Express Forwarding Event Trace Messages*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| This table is intentionally left blank because no features were introduced or modified in Cisco IOS XE Release 2.1 or later. This table will be updated when feature information is added to this module. | -- | -- |

# Glossary

**adjacency** --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

**Cisco Express Forwarding** --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

**distributed Cisco Express Forwardin** g--A mode of Cisco Express Forwarding operation in which line cards maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Processor of involvement in the switching operation.

**FIB** --forwarding information base. A component of Cisco Express Forwarding that is conceptually similar to a routing table or information base. The router uses the FIB lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The router maintains a mirror image of the forwarding information in an IP routing table.

**line card** --A general term for an interface processor that can be used in various Cisco products.

**prefix** --The network address portion of an IP address. A prefix is specified by a network and mask and is generally represented in the format network/mask. The mask indicates which bits are the network bits. For example, 1.0.0.0/16 means that the first 16 bits of the IP address are masked, making them the network bits. The remaining bits are the host bits. In this example, the network number is 10.0.

**VPN** --Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** --A Virtual Private Network (VPN) routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

CHAPTER 11

# SNMP CEF-MIB Support

The Cisco Express Forwarding--SNMP CEF-MIB Support feature introduces the CISCO-CEF-MIB, which allows management applications through the use of the Simple Network Management Protocol (SNMP) to configure and monitor Cisco Express Forwarding operational data and to provide notification when Cisco Express Forwarding encounters specific configured events. This module describes how to use the CISCO-CEF-MIB to manage and monitor objects related to Cisco Express Forwarding operation.

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks: those that carry small amounts of traffic and those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

## Prerequisites for SNMP CEF-MIB Support

- Cisco Express Forwarding or distributed Cisco Express Forwarding must be configured on your system.
- The enhanced Cisco Express Forwarding infrastructure introduced in Cisco IOS XE, Release 2.1 must be included in the image on your system.

- The router on which the Cisco Express Forwarding--SNMP CEF-MIB Support features is to be used must be configured for SNMP access. See the Configuring the Router to Use SNMP, on page 146 of this document for more information.

# Information About SNMP CEF-MIB Support

## CEF Functional Overview

Cisco Express Forwarding is an advanced Layer 3 IP switching technology. It uses a Forwarding Information Base (FIB) to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are propagated to the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. The two main components of Cisco Express Forwarding operation are the FIB and adjacency tables.

Cisco Express Forwarding uses adjacency tables to prepend Layer 2 addressing information. An adjacency table maintains Layer 2 next-hop addresses for all FIB entries. Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. Cisco Express Forwarding discovers and solves adjacencies and populates the adjacency tables.

**Note** The CISCO-CEF-MIB prefix database and its related database can be very large. Therefore, executing a command that displays the prefix table could take a considerable amount of time.

## Benefits of CISCO-CEF-MIB

Command-line interface (CLI) **show** commands are available to obtain Cisco Express Forwarding operational information. Managing Cisco Express Forwarding using the CLI can be a time-consuming task. The increasing capacity of Cisco routers makes parsing the **show** commands output to obtain the needed Cisco Express Forwarding operational parameters more and more difficult.

The CISCO-CEF-MIB allows you to manage and monitor the Cisco Express Forwarding operation using SNMP. In addition, you can configure SNMP to notify you if Cisco Express Forwarding encounters errors.

The CISCO-CEF-MIB introduced with the Cisco Express Forwarding--SNMP CEF-MIB Support feature gives you real-time access to operational information stored in the FIB and adjacency tables, switching statistics, and information on resource failures. The feature enables you to configure parameters related to Cisco Express Forwarding features by utilizing a MIB implementation based on SNMP. This information is accessed using **get** and **set** commands entered on the network management system (NMS) workstation or host system for which SNMP has been implemented. The NMS workstation is also known as the SNMP manager.

Cisco Express Forwarding is available in all Cisco routers. However, CISCO-CEF-MIB support of Cisco Express Forwarding management is dependent on the infrastructure introduced in Cisco IOS XE, Release 2.1.

The implementation of the CISCO-CEF-MIB in Cisco IOS XE, Release 2.1 manages Cisco Express Forwarding instances running on the Route Processor (RP). Information about Cisco Express Forwarding running on the line cards is available to the RP in reference to Cisco Express Forwarding peers only.

The CISCO-CEF-MIB supports configuration and monitoring for both IP versions, IP Version 4 (IPv4) and IP Version 6 (IPv6).

# Information Managed by the CISCO-CEF-MIB

SNMP has historically been used to collect network information. SNMP permits retrieval of critical information from network elements such as routers, switches, and workstations.

The CISCO-CEF-MIB provides managed objects that enable a network administrator to monitor the following:

- Cisco Express Forwarding administrative and operational states as displayed in the output of the **show ip cef summary** command
- Notifications for Cisco Express Forwarding events: Cisco Express Forwarding state changes, Cisco Express Forwarding failures (with a predefined reason), and Route Processor (RP) and line card inconsistencies
- Parameters related to Cisco Express Forwarding for the associated interface as displayed by the **show cef interface** command
- Line card Cisco Express Forwarding states and line card Cisco Express Forwarding FIB states in the Linecard table as displayed by the **show cef linecard**command
- Cisco Express Forwarding statistics: switching statistics, punt counters and punt-to-host counters as displayed by the **show ip cef switching stats**command, and per-prefix counters and nonrecursive counters
- IPv4 and IPv6 notification, when Cisco Express Forwarding is switched between disable and enable and between Cisco Express Forwarding and distributed Cisco Express Forwarding

The SNMP CISCO-CEF-MIB provides managed objects that enable a network administrator to configure the following:

- Cisco Express Forwarding and distributed Cisco Express Forwarding administration status
- Cisco Express Forwarding accounting-related parameters
- Cisco Express Forwarding load sharing-related parameters
- Traffic-related configuration parameters

# CISCO-CEF-MIB Object Groups

The SNMP CISCO-CEF-MIB allows the configuration and management of objects related to Cisco Express Forwarding. The MIB contains the following object groups:

- CEF FIB group
- CEF Adjacency group
- CEF Forwarding Element group
- CEF Cfg group
- CEF Interface group
- CEF Peer group

- CEF Consistency (CC) group
- CEF State Group
- CEF Notification Control group

In the CISCO-CEF-MIB, configuration objects are defined as read-write, and the other objects are defined as read only.

The CISCO-CEF-MIB contains tables related to the Cisco Express Forwarding object groups. These tables provide information about prefixes, forwarding paths, adjacencies, output chain elements (OCEs), prefix-based statistics, information about Cisco Express Forwarding configuration, consistency checkers, switching statistics, and managed objects specific to line card-specific.

The CISCO-CEF-MIB also defines Cisco Express Forwarding notifications that you can enable or disable through the MIB or CLI commands.

The index for most tables in the CISCO-CEF-MIB is entPhysicalIndex.

# CISCO-CEF-MIB Tables

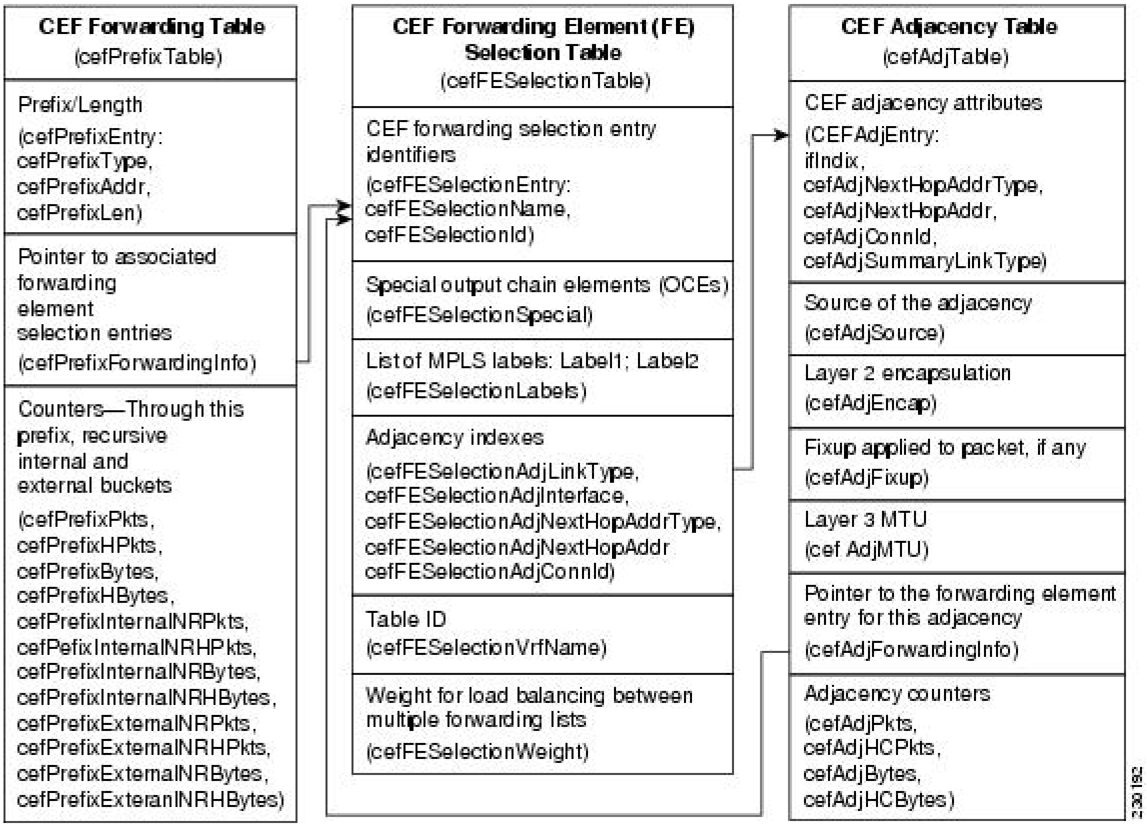
- The CEF FIB Summary table (cefFIBSummaryTable) contains the number of forwarding prefixes for both IPv4 and IPv6 protocols. It is a summary of the CEF Forwarding table.
- The CEF Forwarding table (cefPrefixTable) lists all the prefixes and related counters. It also contains a pointer to the CEF Forwarding Element Selection table.
- The CEF Longest Match Prefix table (cefLMPrefixTable) returns the longest prefix match for the given destination address. An optional cefLMPrefixSpinLock object is provided to reduce conflict in instances when more than one application acts on the CEF Longest Match Prefix table.
- The CEF Path table (cefPathTable) lists all the Cisco Express Forwarding paths.
- The CEF Adjacency Summary table (cefAdJSummaryTable) contains the total number of complete, incomplete, fixup, and redirect adjacencies for all link types.
- The CEF Adjacency table (cefAdjTable) lists all the adjacencies. It contains the adjacency source, encapsulation string, fixup, and Layer 3 maximum transmission unit (MTU) associated with the adjacency entry. It contains a pointer to the forwarding element selection table (if the adjacency is a MID chain adjacency).
- The CEF Forwarding Element Selection table (cefFESelectionTable) represents the OCE chains in flattened format. This table shows only the labels, table ID, and adjacency traversed in the OCE chain. It also contains the weight associated with each OCE chain.
- CEF Cfg table (cefCfgTable) contains all the global configuration parameters related to Cisco Express Forwarding: administration and operational status, accounting-related configuration parameters, load-sharing algorithms and IDs, and traffic statistics parameters.
- CEF Resource table (cefResourceTable) contains information about resources for Cisco Express Forwarding: the memory status of the process memory pool and reasons for the Cisco Express Forwarding resource failure notifications.
- CEF Interface table (cefIntTable) contains the interface-specific Cisco Express Forwarding parameters: interface switching state, interface load sharing (per packet and per destination), and interface nonrecursive routing (internal and external).

- CEF Peer table or Linecard table (cefPeerTable) contains Cisco Express Forwarding information related to peers on a managed line card: line card operational state and the number of times the line card session resets.
- CEF Peer FIB table (cefPeerFIBTable) contains information about the operational state of the Forwarding Information Bases (FIBs) on each line card.
- The CEF Prefix Length Statistics table (cefStatsPrefixTable) maintains prefix length-based statistics.
- CEF Switching Statistics table (cefSwitchingStatsTable) contains the switching statistics for each switching path: drop counters, punt counters, and punt-to-host counters.
- CEF IP Prefix Consistency Checker Global group (cefCCGlobalTable) contains all global configuration parameters for the consistency checkers: auto repair, enable and disable, delay, and hold down; enable or disable the passive consistency checkers; enable or disable the error messages for consistency detection; and the mechanism to activate the full scan consistency checkers. This table also displays the state of full scan consistency checkers.
- CEF Consistency Checker Type table (cefCCTypeTable) contains the consistency checker type specific parameters: frequency and count of scan for passive scanners and the queries sent, ignored, checked, and iterated.
- CEF Inconsistency Record table (cefInconsistencyRecordTable) contains the detected inconsistency records: prefix address and length, table ID, consistency checker type, slot ID, and the reason for the inconsistency (missing or checksum error).

See theOperations Available Through the CISCO-CEF-MIB, on page 138 for information about the specific objects available through the CISCO-CEF-MIB tables.

The figure below shows the contents of the CISCO-CEF-MIB main tables and the relationships of the tables to one another.

*Figure 6: CISCO-CEF-MIB Main Tables, Table Contents, and Relationships*


CEF Forwarding Table
(cefPrefixTable)
Prefix/Length
(cefPrefixEntry: cefPrefixType, cefPrefixAddr, cefPrefixLen)
Pointer to associated forwarding element selection entries
(cefPrefixForwardingInfo)
Counters—Through this prefix, recursive internal and external buckets
(cefPrefixPkts, cefPrefixHPkts, cefPrefixBytes, cefPrefixHBytes, cefPrefixInternalNRPkts, cefPefixInternalNRHPkts, cefPrefixInternalNRBytes, cefPrefixInternalNRHBytes, cefPrefixExternalNRPkts, cefPrefixExternalNRHPkts, cefPrefixExternalNRBytes, cefPrefixExteranINRHBytes)
CEF Forwarding Element (FE) Selection Table
(cefFESelectionTable)
CEF forwarding selection entry identifiers
(cefFESelectionEntry: cefFESelectionName, cefFESelectionId)
Special output chain elements (OCEs)
(cefFESelectionSpecial)
List of MPLS labels: Label1; Label2
(cefFESelectionLabels)
Adjacency indexes
(cefFESelectionAdjLinkType, cefFESelectionAdjInterface, cefFESelectionAdjNextHopAddrType, cefFESelectionAdjNextHopAddr cefFESelectionAdjConnId)
Table ID
(cefFESelectionVrfName)
Weight for load balancing between multiple forwarding lists
(cefFESelectionWeight)
CEF Adjacency Table
(cefAdjTable)
CEF adjacency attributes
(CEFAdjEntry: ifIndix, cefAdjNextHopAddrType, cefAdjNextHopAddr, cefAdjConnId, cefAdjSummaryLinkType)
Source of the adjacency
(cefAdjSource)
Layer 2 encapsulation
(cefAdjEncap)
Fixup applied to packet, if any
(cefAdjFixup)
Layer 3 MTU
(cef AdjMTU)
Pointer to the forwarding element entry for this adjacency
(cefAdjForwardingInfo)
Adjacency counters
(cefAdjPkts, cefAdjHCPkts, cefAdjBytes, cefAdjHCBytes)
230192

# Operations Available Through the CISCO-CEF-MIB

You can use SNMP **get**and **set**commands to configure and monitor Cisco Express Forwarding operations that are available through the CISCO-CEF-MIB tables. This section describes the configuration and monitoring operations for each table.

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF FIB Summary table (cefFIBSummaryTable).

*Table 18: CEF FIB Summary Table--Cisco Express Forwarding Operation and Associated MIB Object*

| Cisco Express Forwarding Operation | Description |
|---|---|
| Gets the number of forwarding prefixes for IPv4 and IPv6 | cefFIBSummaryFwdPrefixes |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Forwarding table (cefPrefixTable).

*Table 19: CEF Forwarding Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Gets the forwarding information for the entry | cefPrefixForwardingInfo |

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Gets the number of packets forwarded by the prefix | cefPrefixPkts |
| Gets the number of packets forwarded by the prefix in a 64-bit value | cefPrefixHCPkts |
| Gets the number of bytes forwarded by the prefix | cefPrefixBytes |
| Gets the number of bytes forwarded by the prefix in a 64-bit value | cefPrefixHCBytes |
| Gets the number of internal nonrecursive packets forwarded by the prefix | cefPrefixInternalNRPkts |
| Gets the number of internal nonrecursive packets forwarded by the prefix in a 64-bit value | cefPrefixInternalNRHCPkts |
| Gets the number of internal nonrecursive bytes forwarded by the prefix | cefPrefixInternalNRBytes |
| Gets the number of internal nonrecursive bytes forwarded by the prefix in a 64-bit value | cefPrefixInternalNRHCBytes |
| Gets the number of external nonrecursive packets forwarded by the prefix | cefPrefixExternalNRPkts |
| Gets the number of external nonrecursive packets forwarded by the prefix in a 64-bit value | cefPrefixExternalNRHCPkts |
| Gets the number of external nonrecursive bytes forwarded by the prefix | cefPrefixExternalNRBytes |
| Gets the number of external nonrecursive bytes forwarded by the prefix in 64-bit value | cefPrefixExternalNRHCBytes |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Longest Match Prefix table (cefLMPrefixTable).

*Table 20: CEF Longest Match Prefix Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Gets or sets the lock for creation or modification of the longest match prefix entries | cefLMPrefixSpinLock |
| Gets the state of the destination prefix request | cefLMPrefixState |
| Gets the network prefix address for the destination prefix request | cefLMPrefixAddr |
| Gets the network prefix length for the destination prefix request (the same display as the **show ip cef exact-route** command) | cefLMPrefixLen |
| Gets the status of a table entry | cefLMPrefixRowStatus |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Path table (cefPathTable).

*Table 21: CEF Path Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Gets the type of Cisco Express Forwarding path for a prefix | cefPathType |
| Gets the interface associated with this Cisco Express Forwarding path | cefPathInterface |
| Gets the next-hop address for the Cisco Express Forwarding path | cefPathNextHopAddr |
| Gets the recursive Virtual Private Network (VPN) routing and forwarding (VRF) instance name associated with this path | cefPathRecurseVrfName |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Adjacency Summary table (cefAdjSummaryTable).

*Table 22: CEF Adjacency Summary Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Gets the number of complete adjacencies | cefAdjSummaryComplete |
| Gets the number of incomplete adjacencies | cefAdjSummaryInComplete |
| Gets the number of adjacencies for Layer 2 encapsulation | cefAdjSummaryFixup |
| Gets the number of adjacencies for IP redirect | cefAdjSummaryRedirect |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Adjacency table (cefAdjTable).

*Table 23: CEF Adjacency Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Gets the adjacency source | cefAdjSource |
| Gets the adjacency Layer 2 encapsulation | cefAdjEncap |
| Gets the adjacency fixup | cefAdjFixup |
| Gets the Layer 3 maximum transmission unit (MTU) for the adjacency | cefAdjMTU |
| Gets the forwarding information in cefFESelectionTable | cefAdjForwardingInfo |
| Gets the number of packets transmitted | cefAdjPkts |
| Gets the number of packets transmitted in a 64-bit version | cefAdjHCPkts |
| Gets the number of bytes transmitted | cefAdjBytes |
| Gets the number of bytes transmitted in a 64-bit version | cefAdjHCBytes |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Forwarding Element Selection table (cefFESelectionTable).

*Table 24: CEF Forwarding Element Selection Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Gets any special processing for a forwarding element | cefFESelectionSpecial |
| Gets the Multiprotocol Label Switching (MPLS) labels for a forwarding element | cefFESelectionLabels |
| Gets the adjancency type for a forwarding element | cefFESelectionAdjLinkType |
| Gets the interface for the adjacency for a forwarding element | cefFESelectionAdjInterface |
| Gets the next-hop address type for the adjacency for a forwarding element | cefFESelectionAdjNextHopAddrType |
| Gets the next-hop address for the adjacency for a forwarding element | cefFESelectionAdjNextHopAddr |
| Gets the connection ID for the adjacency for a forwarding element | cefFESelectionAdjConnId |
| Gets the VRF name for the lookup for a forwarding element | cefFESelectionVrfName |
| Gets the weighting for load balancing for a forwarding element | cefFESelectionWeight |

The table below lists the Cisco Express Forwarding configuration and monitoring operations and associated MIB objects provided by the CEF Cfg table (cefCfgTable).

*Table 25: CEF Cfg Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Enables or disables a Cisco Express Forwarding instance | cefCfgAdminState |
| Queries a Cisco Express Forwarding operational instance | cefCfgOperState |
| Enables or disables a distributed Cisco Express Forwarding instance | cefCfgDistributionAdminState |
| Queries a distributed Cisco Express Forwarding operational instance | cefCfgDistributionOperState |
| Gets or sets Cisco Express Forwarding network accounting options | cefCfgAccountingMap<br>• nonRecursive (0)<br>• perPrefix (1)<br>• prefixLength (2) |
| Gets or sets Cisco Express Forwarding load sharing algorithm options | cefCfgLoadSharingAlgorithm<br>• none (1) - Load sharing is disabled.<br>• original (2)<br>• tunnel (3)<br>• universal (4) |

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Gets or sets a load sharing ID | cefCfgLoadSharingID |
| Gets or sets a traffic interval timer for Cisco Express Forwarding traffic statistics | cefCfgTrafficStatsLoadInterval |
| Gets or sets a frequency timer for the line card to send traffic statistics to the RP | cefCfgTrafficStatsUpdateRate |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Resource table (cefResourceTable).

*Table 26: CEF Resource Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Gets the memory status of process memory pool for Cisco Express Forwarding | cefResourceMemoryUsed |
| Gets the reason for the Cisco Express Forwarding resource failure notification | cefResourceFailureReason |

The table below lists the Cisco Express Forwarding configuration and monitoring operations and associated MIB objects provided by the CEF Interface table (cefIntTable).

*Table 27: CEF Interface Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Gets or sets the Cisco Express Forwarding switching state of the interface | cefIntSwitchingState<br>• cefEnabled (1)<br>• distCefEnabled (2)<br>• cefDisabled (3) |
| Gets or sets the type of Cisco Express Forwarding Load sharing on the interface | cefIntLoadSharing<br>• perPacket (1)<br>• perDestination (2) |
| Gets or sets Cisco Express Forwarding nonrecursive accounting on the interface | cefIntNonrecursiveAccouting<br>• internal (1)<br>• external (2) |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Peer table (or Linecard table) (cefPeerTable).

*Table 28: CEF Peer Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Gets the Cisco Express Forwarding operational instance of the peer entity | cefPeerOperState |
| Gets how many times the session with the Peer resets | cefPeerNumberOfResets |

The table below lists the Cisco Express Forwarding monitoring operation and associated MIB object provided by the CEF Peer FIB table (cefPeerFIBTable).

*Table 29: CEF Peer FIB Table--Cisco Express Forwarding Operation and Associated MIB Object*

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Gets the current Cisco Express Forwarding FIB operation state of the peer entity | cefPeerFIBOperState |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Prefix Length Statistics table (cefStatsPrefixTable).

*Table 30: CEF Prefix Length Statistics Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Gets the number of queries (lookups) in the FIB database for a prefix length | cefStatsPrefixQueries |
| Gets the number of queries (lookups) in the FIB database for a prefix length in a 64-bit value | cefStatsPrefixHCQueries |
| Gets the number of inserts in the FIB database for a prefix length | cefStatsPrefixInserts |
| Gets the number of inserts in the FIB database for a prefix length in a 64-bit value | cefStatsPrefixHCInsert |
| Gets the number of deletes in the FIB database for a prefix length | cefStatsPrefixDeletes |
| Gets the number of deletes in the FIB database for a prefix length in a 64-bit version | cefStatsPrefixHCDeletes |
| Gets the number of elements in the FIB database for a prefix length | cefStatsPrefixElements |
| Gets the number of elements in the FIB database for a prefix length in a 64-bit value | cefStatsPrefixHCElements |

The table below lists the Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Switching Statistics table (cefSwitchingStatsTable).

*Table 31: CEF Switching Statistics Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Gets the switching path of a Cisco Express Forwarding instance | cefSwitchingPath |
| Gets the number of packets dropped by a Cisco Express Forwarding instance | cefSwitchingDrop |

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Gets the number of packets dropped by a Cisco Express Forwarding instance in a 64-bit value | cefSwitchingHCDrop |
| Gets the number of packets that could be punted | cefSwitchingPunt |
| Gets the number of packets that could be punted in a 64-bit value | cefSwitchingHCPunt |
| Gets the number of packets that are punted to the host | cefSwitchingPunt2Host |
| Gets the number of packets that are punted to the host in a 64-bit value | cefSwitchingHCPunt2Host |

The table below lists the Cisco Express Forwarding configuration and monitoring operations and associated MIB objects provided by the CEF IP Prefix Consistency Global Checker group (cefCCGlobalTable).

***Table 32: CEF IP Prefix Consistency Global Checker Group--Cisco Express Forwarding Operations and Associated MIB Objects***

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Enables or disables auto repairing of the consistency checkers | cefCCGlobalAutoRepairEnabled |
| Gets or sets the consistency checker wait time before fixing the inconsistency | cefCCGlobalAutoRepairDelay |
| Gets or sets the consistency checker wait time to reenable auto repair after auto repair runs | cefCCGlobalAutoRepairHoldDown |
| Enables or disables error message generation for an inconsistency | cefCCGlobalErrorMsgEnabled |

The table below lists the Cisco Express Forwarding configuration and monitoring operations and associated MIB objects provided by the CEF Consistency Checker Type table (cefCCTypeTable).

***Table 33: CEF Consistency Checker Type Table--Cisco Express Forwarding Operations and Associated MIB Objects***

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Enables or disables the passive consistency checker | cefCCEnabled |
| Gets or sets the maximum number of prefixes per scan | cefCCCount |
| Gets or sets the period between scans for the consistency checker | cefCCPeriod |
| Gets the number of prefix consistency queries sent to the Cisco Express Forwarding FIB | cefCCQueriesSent |
| Gets the number of prefix consistency queries ignored by the consistent checker | cefCCQueriesIgnored |
| Gets the number of prefix consistent queries iterated back to the database | cefCCQueriesIterated |
| Gets the number of prefix consistent queries processed | cefCCQueriesChecked |

The table below lists the Cisco Express Forwarding configuration and monitoring operations and associated MIB objects provided by the CEF Inconsistency Record table (cefInconsistencyRecordTable).

*Table 34: CEF Inconsistency Record Table--Cisco Express Forwarding Operations and Associated MIB Objects*

| Cisco Express Forwarding Operation | MIB Objects |
|---|---|
| Gets the network prefix type for the inconsistency | cefInconsistencyPrefixType |
| Gets the network prefix address for the inconsistency | cefInconsistencyPrefixAddr |
| Gets the network prefix length for the inconsistency | cefInconsistencyPrefixLen |
| Gets the VRF name for the inconsistency | cefInconsistencyVrfName |
| Gets the consistency checker type that found the inconsistency | cefInconsistencyCCType |
| Gets the entity in which this inconsistency occurred | cefInconsistencyEntity |
| Gets the reason for generating the inconsistency | cefInconsistencyReason<br>• missing (1)<br>• checksumErr (2)<br>• unknown (3) |
| Global Objects for Cisco Express Forwarding Inconsistency | entLastInconsistencyDetectTime |
| Gets the value of the system uptime at the time an inconsistency was detected | |
| Sets an object to restart all active consistency checkers | cefInconsistencyReset |
| Gets the status of the inconsistency reset request | cefInconsistencyResetStatus |

# CISCO-CEF-MIB Notifications

The table below lists the Cisco Express Forwarding operations associated with the CISCO-CEF-MIB objects that enable the sending of Cisco Express Forwarding notifications.

*Table 35: Cisco Express Forwarding Notifications--Cisco Express Forwarding Operations and CISCO-CEF-MIB Objects That Enable Them*

| Cisco Express Forwarding Operation | MIB Object |
|---|---|
| Enables the sending of a notification on the detection of a Cisco Express Forwarding resource failure | cefResourceFailureNotifEnable |
| Enables the sending of a notification on the detection of a Cisco Express Forwarding peer state change | cefPeerStateChangeNotifEnable |
| Enables the sending of a notification on the detection of a Cisco Express Forwarding FIB peer state change | cefPeerFIBStateChangeNotifEnable |
| Sets the period of time after the sending of each notification event | cefNotifThrottlingInterval |
| Enables the sending of a notification on the detection of an inconsistency | cefInconcsistencyNotifEnable |

You can enable or disable these notifications through the MIB or by entering a CLI command. The table below contains a description of the notifications and the commands you use to enable each notification.

**Note** You must enter a **snmp-server host** command before you enter a command to enable or disable a CISCO-CEF-MIB notification.

*Table 36: Description of Notifications and Enabling Commands for the CEF-PROVISION-MIB Notifications*

| Notification | Generated for | Commands |
|---|---|---|
| Cisco Express Forwarding resource failure notification | A malloc failure, an Inter-Process Communication (IPC) failure, and any other type of failure related to External Data Representation (XDR) messages | CLI: **snmp-server enable traps cef resource-failure**<br>MIB: **setany** *version ip-address community-string* **cefResourceFailureNotifEnable.0 -i 1** |
| Cisco Express Forwarding peer state change notification | A change in the operational state of a peer on the line cards | CLI: **snmp-server enable traps cef peer-state-change**<br>MIB: **setany** *version ip-address community-string* **cefPeerStateChangeNotifEnable.0 -i 1** |
| Cisco Express Forwarding peer FIB state change notification | A change in the operational state of the peer FIB | CLI: **snmp-server enable traps cef peer-fib-state-change**<br>MIB: **setany** *version ip-address community-string* **cefPeerFIBStateChangeNotifEnable.0 -i 1** |
| Cisco Express Forwarding inconsistency detection notification | An inconsistency detected by the consistency checkers | CLI: **snmp-server enable traps cef inconsistency**<br>MIB: **setany** *version ip-address community-string* **cefInconsistencyNotifEnable.0 -i 1** |

# How to Configure SNMP CEF-MIB Support

## Configuring the Router to Use SNMP

Perform the following task to configure a router to use SNMP.

Before you can use the Cisco Express Forwarding--SNMP CEF-MIB Support feature, you must configure the SNMP server for the router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6 nacl**] [*access-list-number*]
4. **snmp-server community** *string2* **rw**
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server community** *string* [**view** *view-name*] [**ro** \| **rw**] [**ipv6 nacl**] [*access-list-number*]<br>**Example:**<br>`Router(config)# snmp-server community public ro` | Sets up the community access string to permit access to SNMP.<br>- The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string.<br>- The **view** *view-name* keyword-argument pair is the name of a previously defined view. The view defines the objects available to the SNMP community.<br>- The **ro** keyword specifies read-only access. Authorized management stations can only retrieve MIB objects.<br>- The **rw** keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects.<br>- The **ipv6 nacl**keywords specify the IPv6 named access list.<br>- The *access-list-number* argument is an integer from 1 to 99. It specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses that are allowed access to the SNMP agent.<br>Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers. Devices at these addresses are allowed to use the community string to gain access to the SNMP agent. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** The *string*argument (Step 3) and *string2*argument (Step 4) provide a minimal level of security. It is advisable to provide the string for read-only access to others who need only to view and not to modify the MIB objects, and reserve the read-write access string for administrators only. The *string2* argument (Step 4) should be different from the read-only *string* argument specified in this step. |
| **Step 4** | **snmp-server community** *string2* **rw**<br>**Example:**<br>`Router(config)# snmp-server community private rw` | Sets up the community access string to permit access to SNMP.<br>• The *string2* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string.<br>• The **rw** keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects.<br>This example allows MIB objects to be retrieved and set because a string is specified with read-write access.<br>**Note** The *string*argument (Step 3) and *string2*argument (Step 4) provide a minimal level of security. It is advisable to provide the string for read-only access to others who need only to view and not to modify the MIB objects, and reserve the read-write access string for administrators only. The *string2* argument (Step 4) should be different from the read-only *string* argument specified in the preceding step (Step 3). |
| **Step 5** | **end**<br>**Example:**<br>`Router(config)# end` | Exits to privileged EXEC mode. |

# Configuring a Host to Receive Notifications

Perform the following task to configure an SNMP host to receive CISCO-CEF-MIB notifications. Notifications provide information to assist you in the monitoring and managing of Cisco Express Forwarding operations.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* [**ro** | **rw**]
4. **snmp-server community** *string2* **rw**
5. **snmp-server host** *ip-address* [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1**| **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] **cef**
6. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server community** *string* [**ro** \| **rw**]<br>**Example:**<br>`Router(config)# snmp-server community public ro` | Sets up the community access string to permit access to SNMP.<br>• The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string.<br>• The **ro** keyword specifies read-only access. Authorized management stations can only retrieve MIB objects.<br>• The **rw** keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects. |
| **Step 4** | **snmp-server community** *string2* **rw**<br>**Example:**<br>`Router(config)# snmp-server community private rw` | Sets up the community access string to permit access to SNMP.<br>• The *string2* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string.<br>• The **rw** keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects. |

| | Command or Action | Purpose |
|---|---|---|
| | | This example allows MIB objects to be retrieved and set because a string is specified with read-write access.<br>**Note** The *string*argument (Step 3) and *string2*argument (Step 4) provide a minimal level of security. It is advisable to provide the string for read-only access to others who need only to view and not to modify the MIB objects, and retain the read-write access string for administrators only. The *string2* argument (Step 4) should be different from the read-only *string* argument specified in the preceding step (Step 3). |
| **Step 5** | **snmp-server host** *ip-address* [**vrf** *vrf-name*] [**traps** \| **informs**] [**version** {**1**\| **2c** \| **3** [**auth** \| **noauth** \| **priv**]}] *community-string* [**udp-port** *port*] **cef**<br>**Example:**<br>`Router(config)# snmp-server host 10.56.125.47 informs version 2c public cef` | Specifies the recipient of an SNMP notification operation.<br>• The *ip-address* argument is the IP address or IPv6 address of the SNMP notification host.<br>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.<br>• The **vrf** *vrf-name* keyword and argument specify that the specified VRF be used to send SNMP notifications.<br>• The **traps** keyword specifies that notifications should be sent as traps. This is the default.<br>• The **informs** keyword specifies that notifications should be sent as informs.<br>• The version keyword specifies the version of the SNMP used to send the traps. The default is 1.<br>If you use the **version** keyword, one of the following keywords must be specified:<br>• • **1** --SNMPv1. This option is not available with informs.<br>• **2c** --SNMPv2c.<br>• **3** --SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**.<br>• One of the following three optional security level keywords can follow the **version 3** keywords:<br>• **auth**--Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. |

| | Command or Action | Purpose |
|---|---|---|
| | | • **noauth**--Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.<br>• **priv**--Enables Data Encryption Standard (DES) packet encryption (also called "privacy").<br>• The *community-string* argument specifies that a password-like community string be sent with the notification operation.<br>• The **udp-port** *port* keyword and argument specify that SNMP notifications or informs are to be sent to the User Datagram Protocol (UDP) port number of the NMS host. The default is 162.<br>• The **cef** keyword specifies that the Cisco Express Forwarding notification type is to be sent to the host. If no type is specified, all available notifications are sent. |
| **Step 6** | **end**<br>**Example:**<br>`Router(config)# end` | Exits to privileged EXEC mode. |

# Configuring SNMP Notifications with the CLI

Perform the following task to configure SNMP notifications for Cisco Express Forwarding events. To configure this feature using SNMP commands instead of the CLI, see the Configuring SNMP Notifications with SNMP Commands, on page 153.

### Before you begin

You must have configured an NMS or SNMP agent to receive the SNMPCISCO-CEF-MIB notification. See the Configuring a Host to Receive Notifications, on page 148.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps cef** [**peer-state-change**] [**resource-failure**] [**inconsistency**] [**peer-fib-state-change**]
4. **snmp-server host** *ip-address* [**traps** | **informs**] [**version** {**1**| **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* **cef**
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server enable traps cef** [**peer-state-change**] [**resource-failure**] [**inconsistency**] [**peer-fib-state-change**]<br>**Example:**<br>`Router(config)# snmp-server enable traps cef resource-failure` | Enables Cisco Express Forwarding support of SNMP notifications on an NMS.<br>- The **peer-state change** keyword enables the sending of CISCO-CEF-MIB SNMP notifications for changes in the operational state of Cisco Express Forwarding peers.<br>- The **resource-failure** keyword enables the sending of CISCO-CEF-MIB SNMP notifications for resource failures that affect Cisco Express Forwarding operations.<br>- The **inconsistency**keyword enables the sending of CISCO-CEF-MIB SNMP notifications for inconsistencies that occur when routing information is updated from the Routing Information Base (RIB) to the CISCO-CEF-MIB on the RP and to the CISCO-CEF-MIB on the line cards.<br>You can set the throttling interval for sending inconsistency notifications. See the Configuring the Throttling Interval with the CLI, on page 155.<br>- The **peer-fib-state-change** keyword enables the sending of CISCO-CEF-MIB SNMP notifications for changes in the operational state of the Cisco Express Forwarding peer FIB. |
| **Step 4** | **snmp-server host** *ip-address* [**traps** \| **informs**] [**version** {**1**\| **2c** \| **3** [**auth** \| **noauth** \| **priv**]}] *community-string* **cef**<br>**Example:**<br>`Router(config)# snmp-server host 10.56.125.47 informs version 2c public cef` | Specifies the recipient of an SNMP notification operation.<br>- The *ip-address* argument is the IP address or IPv6 address of the SNMP notification host.<br>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.<br>- The **traps** keyword specifies that notifications should be sent as traps. This is the default. |

| | Command or Action | Purpose |
|---|---|---|
| | | • The **informs** keyword specifies that notifications should be sent as informs.<br>• The **version** keyword specifies the version of the SNMP used to send the traps or informs. The default is 1.<br>If you use the **version** keyword, one of the following keywords must be specified:<br>• • **1** --SNMPv1. This option is not available with informs.<br>• **2c** --SNMPv2C.<br>• **3** --SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**.<br>• One of the following three optional security level keywords can follow the **version 3** keywords:<br>• **auth**--Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.<br>• **noauth**--Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.<br>• **priv**--Enables Data Encryption Standard (DES) packet encryption (also called "privacy").<br>• The *community-string* argument specifies that a password-like community string be sent with the notification operation.<br>• The **cef** keyword specifies that the Cisco Express Forwarding notification type is to be sent to the host. If no type is specified, all available notifications are sent. |
| **Step 5** | **end**<br>**Example:**<br>`Router(config)# end` | Exits to privileged EXEC mode. |

## Configuring SNMP Notifications with SNMP Commands

Perform the following task to configure SNMP notifications for Cisco Express Forwarding events. To configure this feature using the CLI instead of SNMP commands, see the Configuring SNMP Notifications with the CLI, on page 151.

### Before you begin

You must have configured an NMS or SNMP agent to receive the SNMPCISCO-CEF-MIB notification. See the Configuring a Host to Receive Notifications, on page 148.

## SUMMARY STEPS

1. **setany** *version* *ip-address* *community-string* **cefPeerStateChangeNotifEnable.0** **-i** *TruthValue*
2. **setany** *version* *ip-address* *community-string* **cefPeerFIBStateChangeNotifEnable** **.0** **-i** *TruthValue*
3. **setany** *version* *ip-address* community-string **cefResourceFailureNotifEnable. 0** **-i** *TruthValue*
4. **setany** *version* *ip-address* *community-string* **cefInconsistencyNotifEnable** **.0** **-i** *TruthValue*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **setany** *version* *ip-address* *community-string* **cefPeerStateChangeNotifEnable.0** **-i** *TruthValue*<br>**Example:**<br>`workstation% setany -v2c 10.56.125.47 public cefPeeStateStateChangeNotifEnable.0 -1 1` | Enables the sending of CISCO-CEF-MIB SNMP notifications for changes in operational state of Cisco Express Forwarding peers.<br>• The *version* argument specifies the version of SNMP that is used. Options are<br>  • **-v1**--SNMPv1<br>  • **-v2c**--SNMPv2C<br>  • **-v3**--SNMPv3<br>• The *ip-address* argument is the IP address or IPv6 address of the SNMP notification host.<br>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.<br>• The *community-string* argument specifies that a password-like community string be sent with the notification operation.<br>• The **-i**keywords indicate that the variable that follows is an integer.<br>• Values for the *TruthValue* argument are:<br>  • 1--enable sending of the notification<br>  • 2--disable sending of the notification<br>These arguments and keywords apply to the Cisco-CEF-MIB notifications in Steps 2, 3, and 4. |
| **Step 2** | **setany** *version* *ip-address* *community-string* **cefPeerFIBStateChangeNotifEnable** **.0** **-i** *TruthValue*<br>**Example:**<br>`workstation% setany -v2c 10.56.125.47 public cefPeerFIBStateChangeNotifEnable.0 -1 1` | Enables the sending of CISCO-CEF-MIB SNMP notifications for changes in the operational state of the Cisco Express Forwarding peer FIB.<br>• See Step 1 for a description of the command arguments and keywords. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **setany** *version* *ip-address* community-string **cefResourceFailureNotifEnable. 0** **-i** *TruthValue*<br>**Example:**<br>`workstation% setany -v2c 10.56.125.47 public cefResourceFailureNotifEnable.0 -i 1` | Enables the sending of CISCO-CEF-MIB SNMP notifications for resource failures that affect Cisco Express Forwarding operations.<br>• See Step 1 for a description of the command arguments and keywords. |
| **Step 4** | **setany** *version* *ip-address* *community-string* **cefInconsistencyNotifEnable .0** **-i** *TruthValue*<br>**Example:**<br>`workstation% setany -v2c 10.56.125.47 public cefInconsistencyNotifEnable.0 -i 1` | Enables the sending of CISCO-CEF-MIB SNMP notifications for inconsistencies that occur when routing information is updated from the RIB to the Cisco Express Forwarding FIB on the RP and to the Cisco Express Forwarding FIB on the line cards.<br>• See Step 1 for a description of the command arguments and keywords. |

# Configuring the Throttling Interval with the CLI

Perform the following task to configure the throttling interval for CISCO-CEF-MIB inconsistency notifications. To configure this feature using SNMP commands instead of the CLI, see the Configuring the Throttling Interval with SNMP Commands section.

Configuring a throttling interval allows some time before an inconsistency notification is sent during the process of updating forwarding information from the Routing Information Base (RIB) to the RP and to the line card databases. As these databases are updated, inconsistencies might occur as a result of the asynchronous nature of the distribution mechanism for these databases. The throttling interval allows fleeting inconsistencies to resolve themselves before an inconsistency notification is sent.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps cef inconsistency**
4. **snmp mib cef throttling-interval** *seconds*
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# configure terminal` | |
| **Step 3** | **snmp-server enable traps cef inconsistency**<br>**Example:**<br>`Router(config)# snmp-server enable traps cef inconsistency` | Enables the sending of CISCO-CEF-MIB SNMP notifications for inconsistencies in Cisco Express Forwarding. |
| **Step 4** | **snmp mib cef throttling-interval** *seconds*<br>**Example:**<br>`Router(config)# snmp mib cef throttling-interval 2500` | Sets the throttling interval for the CISCO-CEF-MIB inconsistency notifications.<br>• The *seconds* argument is the time to allow before an inconsistency notification is sent during the process of updating forwarding information from the RIB to the RP and to the line card databases. A valid value is from 0 to 3600 seconds. A value of 0 disables throttle control. |
| **Step 5** | **end**<br>**Example:**<br>`Router(config)# end` | Exits to privileged EXEC mode. |

# Configuring the Throttling Interval with SNMP Commands

Perform the following task to configure the throttling interval for CISCO-CEF-MIB inconsistency notifications. To configure this feature using the CLI instead of SNMP commands, see the Configuring the Throttling Interval with the CLI, on page 155.

Configuring a throttling interval allows some time before an inconsistency notification is sent during the process of updating forwarding information from the Routing Information Base (RIB) to the RP and to the line card databases. As these databases are updated, inconsistencies might occur as a result of the asynchronous nature of the distribution mechanism for these databases. The throttling interval allows fleeting inconsistencies to resolve themselves before an inconsistency notification is sent.

## SUMMARY STEPS

1. **setany** *version* *ip-address* *community-string* **cefNotifThrottlingInterval.0** **-i** *seconds*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **setany** *version* *ip-address* *community-string* **cefNotifThrottlingInterval.0** **-i** *seconds*<br>**Example:**<br>`workstation% setany -v2c 10.56.125.47 public cefNotifThrottlingInterval.0 -1 3600` | Sets the throttling interval for the CISCO-CEF-MIB inconsistency notifications.<br>• The *version* argument specifies the version of SNMP that is used. Options are<br>• **-v1**--SNMPv1 |

| | Command or Action | Purpose |
|---|---|---|
| | | • **-v2c**--SNMPv2C<br>• **-v3**--SNMPv3<br>• The *ip-address* argument is the IP address or IPv6 address of the SNMP notification host.<br>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.<br>• The *community-string* argument specifies that a password-like community string be sent with the notification operation.<br>• The **-i**keywords indicate that the variable that follows is an integer.<br>• The *seconds* argument is the time to allow before an inconsistency notification is sent during the process of updating forwarding information from the RIB to the RP and to the line card databases. A valid value is from 0 to 3600 seconds. A value of 0 disables throttle control. |

# Configuration Examples for SNMP CEF-MIB Support

## Example Configuring a Host to Receive Notifications

The following example shows how to configure an SNMP host to receive CISCO-CEF-MIB notifications:

```
configure terminal
!

snmp-server community public ro

snmp-server community private rw

snmp-server host 10.56.125.47 informs version 2vc public cef

end
```

This example sets up SNMP host 10.56.125.47 to receive CISCO-CEF-MIB notifications as informs.

## Example Configuring SNMP Notifications

This section contains examples for configuring SNMP notifications for Cisco Express Forwarding events using the CLI and using SNMP commands.

### Configuring SNMP Notifications for Cisco Express Forwarding Events Using the CLI

This example shows how to use the CLI to configure CISCO-CEF-MIB SNMP notifications to be sent to host 10.56.125.47 as informs for changes in Cisco Express Forwarding peer states and peer FIB states, for Cisco Express Forwarding resource failures, and for inconsistencies in Cisco Express Forwarding events:

```
configure terminal
!

snmp-server community public ro

snmp-server host 10.56.125.47 informs version 2c public cef

!
snmp-server enable traps cef peer-state-change
snmp-server enable traps cef peer-fib-state-change
snmp-server enable traps cef inconsistency
snmp-server enable traps cef resource-failure
end
```

### Configuring SNMP Notifications for Cisco Express Forwarding Events Using SNMP Commands

This example shows the use of SNMP command to configure CISCO-CEF-MIB SNMP notifications to be sent to host 10.56.125.47 for changes in Cisco Express Forwarding peer states and peer FIB states, for Cisco Express Forwarding resource failures, and for inconsistencies in Cisco Express Forwarding events:

```
setany -v2c 10.56.125.47 public cefPeerStateChangeNotifEnable.0 -i 1

setany -v2c 10.56.125.47 public cefPeerFIBStateChangeNotifEnable.0 -i 1

setany -v2c 10.56.125.47 public cefResourceFailureNotifEnable.0 -i 1
setany -v2c 10.56.125.47 public cefInconsistencyNotifEnabled.0 -i 1
```

## Example Configuring the Throttling Interval

This example shows the configuration of a throttling interval for the sending of Cisco Express Forwarding inconsistency notifications to the SNMP host using CLI commands and SNMP commands. The throttling interval is the amount of time that passes between the time that the inconsistency occurs and the sending of the notification to the SNMP host.

### Configuring the Throttling Interval for CISCO-CEF-MIB Inconsistency Notifications Using CLI Commands

This example shows the addition of a throttling interval of 1000 seconds for the sending of Cisco Express Forwarding inconsistency notifications to the SNMP host using CLI commands:

```
configure terminal
!

snmp-server community public ro

snmp-server host 10.56.125.47 informs version 2c public cef
```

```
!
snmp-server enable traps cef peer-state-change
snmp-server enable traps cef peer-fib-state-change
snmp-server enable traps cef inconsistency
snmp-server enable traps cef resource-failure
!
snmp mib cef throttling-interval 1000
end
```

### Configuring the Throttling Interval for CISCO-CEF-MIB Inconsistency Notifications Using SNMP Commands

This example shows the addition of a throttling interval of 1000 seconds for the sending of Cisco Express Forwarding inconsistency notifications to the SNMP host using an SNMP command:

```
setany -v2c 10.56.125.47 public cefNotifThrottlingInterval.0 -1 1000
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Commands for configuring and managing Cisco Express Forwarding | *Cisco IOS IP Switching Command Reference* |
| Tasks for verifying basic Cisco Express Forwarding and distributed Cisco Express Forwarding operation | Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks |
| Tasks for enabling or disabling Cisco Express Forwarding or distributed Cisco Express Forwarding | Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding to Customize Switching and Forwarding for Dynamic Network |
| Tasks for configuring load-balancing schemes for Cisco Express Forwarding | Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic |
| Tasks for configuring Cisco Express Forwarding consistency checkers | Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards |
| Tasks for configuring epochs for Cisco Express Forwarding tables | Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables |
| Tasks for configuring and verifying Cisco Express Forwarding network accounting | Configuring Cisco Express Forwarding Network Accounting |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| RFC 3291 | *Textual Conventions for Internet Network Addresses* |
| RFC 3413 | *Simple Network Management Protocol (SNMP) Applications* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for SNMP CEF-MIB Support

*Table 37: Feature Information for Cisco Express Forwarding--SNMP CEF-MIB Support*

| Feature Name | Release | Feature Information |
|---|---|---|
| Cisco Express Forwarding--SNMP CEF-MIB Support | Cisco IOS XE Release 2.1 | The Cisco Express Forwarding--SNMP CEF-MIB Support feature introduces the CISCO-CEF-MIB that allows management applications through the use of the Simple Network Management Protocol (SNMP) to configure and monitor Cisco Express Forwarding operational data and to provide notification when Cisco Express Forwarding encounters specific configured events. This module describes how to use the CISCO-CEF-MIB to manage and monitor objects related to Cisco Express Forwarding operation.<br>In Cisco IOS XE, Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br>The following commands were introduced or modified: **snmp mib cef throttling-interval**, **snmp-server enable traps cef**, **snmp-server host**. |

# Glossary

**inform** --A type of notification message that is more reliable than a conventional trap notification message because the informs message notification requires acknowledgment, but a trap notification does not.

**IPC** --Inter-Process Communication. The protocol used by routers that support distributed packet forwarding. The Cisco IOS XE version of IPC provides a reliable ordered delivery of messages using an underlying platform driver transport or User Date Protocol (UDP) transport protocol. Cisco IOS XE software IPC services allow line cards (LCs) and the central route processor (RP) in a distributed system, to communicate with each other by exchanging messages from the RP to the LCs. Communication messages are also exchanged between active and standby RPs. The IPC messages include configuration commands, responses to the configuration commands, and other events that are reported by an LC to the RP.

**MIB** --Management Information Base. A database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP). The value of a MIB object can be changed or retrieved by the use of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**NMS** --network management station. A powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks. In the context of SNMP, an NMS is a device that performs SNMP queries to the SNMP agent of a managed device to retrieve or modify information.

**notification** --A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal to indicate that a significant network event has occurred.

**SNMP** --Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP enables a user to monitor and control network devices, manage configurations, collect statistics, monitor performance, and ensure network security.

**SNMP community** --An authentication scheme that enables an intelligent network device to validate SNMP requests.

**SNMPv2c** --Version 2c of the Simple Network Management Protocol. SNMPv2c supports centralized as well as distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

**SNMPv3** --Version 3 of the Simple Network Management Protocol. Interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

**trap** --A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant network event has occurred. Traps are less reliable than inform requests, because the receiver of the trap does not send an acknowledgment of receipt; furthermore, the sender of the trap cannot determine if the trap was received.

CHAPTER 12

# IPv6 CEF-Switched Tunnels

Cisco Express Forwarding switching can be used for IPv6 manually configured tunnels.

# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

# Information About IPv6 CEF-Switched Tunnels

## IPv6 Manually Configured Tunnels

A manually configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 backbone. The primary use is for stable connections that require regular secure communication between two edge devices or between an end system and an edge device, or for connection to remote IPv6 networks.

An IPv6 address is manually configured on a tunnel interface, and manually configured IPv4 addresses are assigned to the tunnel source and the tunnel destination. The host or device at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks. Manually configured tunnels can be configured between border devices or between a border device and a host. Cisco Express Forwarding switching can be used for IPv6 manually configured tunnels, or Cisco Express Forwarding switching can be disabled if process switching is needed.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| Tunnels | *Interface and Hardware Component Configuration Guide* |
| Cisco IOS commands | *Cisco IOS Master Commands List, All Releases* |
| IPv6 commands | *Cisco IOS IPv6 Command Reference* |
| Cisco IOS IPv6 features | *Cisco IOS IPv6 Feature Mapping* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFCs for IPv6 | *IPv6 RFCs* |

### MIBs

| MIB | MIBs Link |
|---|---|
|  | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

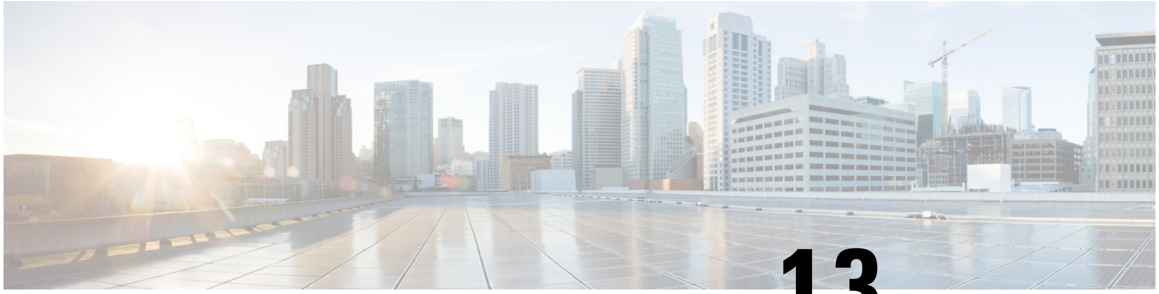
### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for IPv6 CEF-Switched Tunnels

*Table 38: Feature Information for IPv6 CEF-Switched Tunnels*

| Feature Name | Releases | Feature Information |
|---|---|---|
| CEFv6 Switching for 6to4 Tunnels | 12.2(28)SB<br>12.2(25)SG<br>12.2(33)SRA<br>12.2(18)SXE<br>12.2(12)T<br>12.4<br>15.0(1)S<br>Cisco IOS XE 3.9(S) | Cisco Express Forwarding switching can be used for IPv6 manually configured tunnels. |
| IPv6 Switching: CEFv6 Switched Automatic IPv4-Compatible Tunnels | 12.2(2)T<br>12.2(52)SG<br>12.2(33)SRA<br>12.2(17a)SX1<br>Cisco IOS XE 3.9(S) | IPv6 supports this feature. |
| IPv6 Switching: CEFv6 Switched Configured IPv6 over IPv4 Tunnels | 12.2(13)T<br>12.2(52)SG<br>12.2(33)SRA<br>12.2(17a)SX1<br>Cisco IOS XE 3.9(S) | IPv6 supports this feature. |
| IPv6 Switching: CEFv6 Switched ISATAP Tunnels | 12.2(15)T<br>12.2(25)SG<br>3.2.0SG<br>15.0(2)SG<br>12.2(33)SRA<br>12.2(17a)SX1<br>Cisco IOS XE 3.9(S) | IPv6 supports this feature. |



CHAPTER 13

# Load Balancing Application Flows Using Deep Packet Inspection Algorithm

The Deep Packet Inspection (DPI) algorithm helps in identification of application flows to facilitate detailed inspection of packets. The DPI algorithm deeply inspects the packets and therefore helps the service provider identify efficient ways to share bandwidth among parallel ethernet interfaces.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

## Prerequisites for ECMP Loadbalance with Tunnel Visibility

- Enable entropy label feature to compute hashing in Layer 2 Virtual Private Networks (L2VPN) core network.

## Restrictions for ECMP Loadbalance with Tunnel Visibility

- Deep Packet Inspection (DPI) for flow-label in IPv6 is not supported.

- DPI is not supported for fragment traffics.

# Information About Load Balancing Using Deep Packet Inspection Algorithm

## Packet Inspection and Identification Using Hash Value

The DPI algorithm performs deep inspection of packets to generate a unique hash value that helps in identification of packets that flow into parallel links. This helps in effective sharing of bandwidth among subscribers.

**Note** The packet inspection is done for both IPv4 and IPv6 traffic. If the traffic is of type PPoE, then enabling the DPI algorithm performs load balancing of the PPPoE traffic as well.

## Preserve Key Control Configuration

If you choose to remove the DPI configurations, you can do that using the command **no port-channel load-balance-hash-algo dpi algorithm** command. This will remove all the DPI tunnel and key-control configurations.

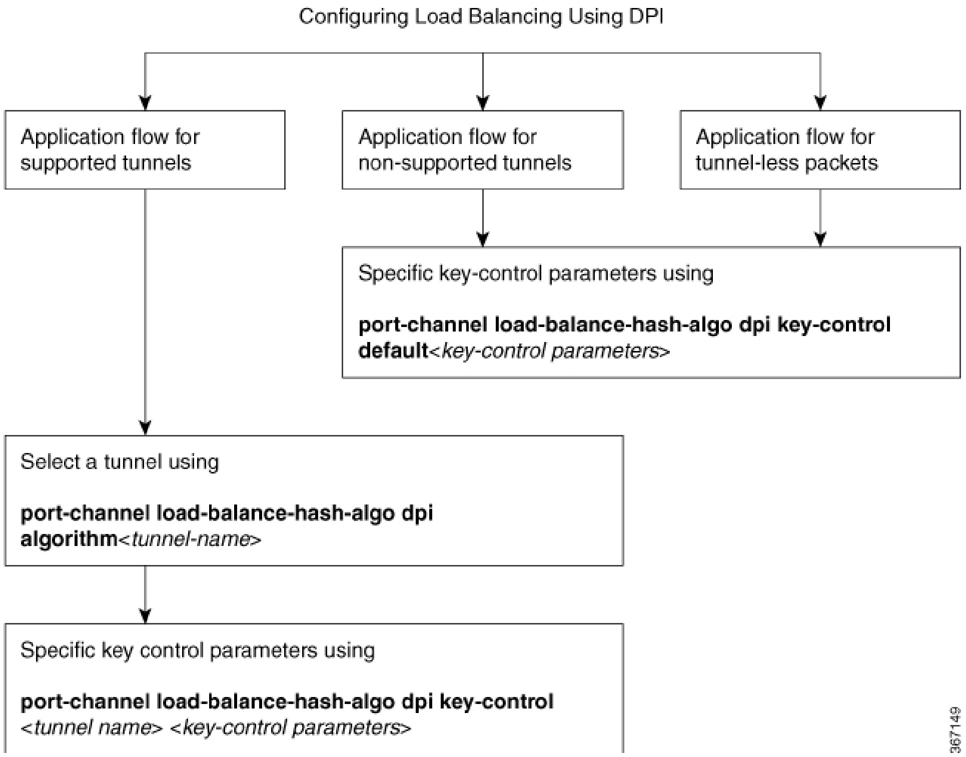
## Support for Tunnel and Tunnel-Less Packets

The DPI algorithm is supported for the following tunnels:

- GRE
- IPsec
- IPinIP
- VxLAN
- In addition to supporting the above mentioned tunnels, DPI can also be performed for tunnel-less packets using **port-channel load-balance-hash-algo dpi key-control default** command.

  When you configure load balancing using DPI you can specify a specific tunnel using the **port-channel load-balance-hash-algo dpi algorithm <tunnel-name>** command. If you prefer to configure DPI for all the tunnels, use the **port-channel load-balance-hash-algo dpi algorithm** command without a tunnel name. This configures DPI for all the tunnels and port-channels.

*Figure 7: Configuring Load Balancing Using DPI*


Configuring Load Balancing Using DPI
Application flow for supported tunnels
Application flow for non-supported tunnels
Application flow for tunnel-less packets
Specific key-control parameters using
**port-channel load-balance-hash-algo dpi key-control default**<*key-control parameters*>
Select a tunnel using
**port-channel load-balance-hash-algo dpi algorithm**<*tunnel-name*>
Specific key control parameters using
**port-channel load-balance-hash-algo dpi key-control** <*tunnel name*> <*key-control parameters*>
367149

# Example: Configuring DPI for IPinIP Tunnel with Key-Control Parameter

```
enable
configure terminal
(config)# port-channel load-balance-hash-algorithm dpi keycontrol tunnel-ipinip
outer-src-dst-ip ignore-inner-ip
ignore-inner-port
```

## Configuring Load Balancing Using Deep Packet Inspection for Tunnel-Based Flow

```
enable
configure terminal
port-channel load-balance-hash-algo dpi algorithm <tunnelname>
port-channel load-balance-hash-algo dpi key-control <tunnel-name> <key-control variables>
end
```

# Examples for Configuring Load Balancing Using for Tunnel-Based Flow

## Example: ECMP Loadbalance with Tunnel Visibility

```
ip cef load-sharing algorithm dpi tunnel-gre tunnel-l2tp tunnel-ipsec tunnel-ipinip
tunnel-vxlan l2vpn-mac
ip cef load-sharing key-control dpi tunnel-gre outer-src-dst-ip inner-src-dst-ip
inner-src-dst-port
ip cef load-sharing key-control dpi tunnel-l2tp outer-src-dst-ip outer-src-dst-port
inner-src-dst-ip inner-src-dst-port
ip cef load-sharing key-control dpi tunnel-ipsec outer-src-dst-ip
ip cef load-sharing key-control dpi tunnel-ipinip outer-src-dst-ip inner-src-dst-ip
inner-src-dst-port
ip cef load-sharing key-control dpi tunnel-vxlan outer-src-dst-ip outer-src-dst-port
inner-src-dst-mac inner-vlan 3
ip cef load-sharing key-control dpi l2vpn-mac outer-src-dst-mac outer-vlan 3 outer-src-dst-ip
 outer-src-dst-port inner-src-dst-mac inner-vlan 3 inner-src-dst-ip inner-src-dst-port
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Load Balancing with DPI Algorithm

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 39: Feature Information for Load Balancing Using DPI Algorithm*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Load Balancing Application Flows Using Deep Packet Inspection | Cisco IOS XE Gibraltar 16.10.1. | The Deep Packet Inspection (DPI)<br>helps in identification of application flows to facilitate detailed inspection of packets. The DPI algorithm deeply inspects the packets and therefore helps the service provider identify efficient ways to share bandwidth among parallel Ethernet interfaces.<br>The following commands were modified:<br>port-channel load-balance-hash-algorithm dpi algorithm. .<br>port-channel load-balance-hash-algorithm dpi key-control. . |