Cisco Express Forwarding—SNMP CEF-MIB Support

First Published: December 4, 2006
Last Updated: December 4, 2006

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 (CEF) operational data and to provide notification when CEF encounters specific configured events. This module describes how to use the CISCO-CEF-MIB to manage and monitor objects related to CEF operation.

CEF 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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Cisco Express Forwarding—SNMP CEF-MIB Support" section on page 41.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Cisco Express Forwarding—SNMP CEF-MIB Support

The Cisco Express Forwarding—SNMP CEF-MIB Support feature has the following prerequisites:

- CEF or distributed CEF (dCEF) must be configured on your system.
- The Cisco Express Forwarding infrastructure introduced in Cisco IOS Release12.2(22)S 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 should be configured for SNMP access. Refer to the "Configuring the Router to Use SNMP" section on page 15 in this document for more information.

Restrictions for Cisco Express Forwarding—SNMP CEF-MIB Support

The CISCO-CEF-MIB prefix database and its related database can be very large. Therefore, walking the prefix table could take a considerable amount of time.

Information About Cisco Express Forwarding—SNMP CEF-MIB Support

To configure SNMP and the CISCO-CEF-MIB to monitor CEF data and events, you should understand the following concepts:

- Cisco Express Forwarding Functional Overview, page 3
- CISCO-CEF-MIB Benefits, page 3
- CEF Information Managed by the CISCO-CEF-MIB, page 3
- CISCO-CEF-MIB Object Groups and Related Tables, page 4
- Brief Description of the Tables in the CISCO-CEF-MIB, page 5

Cisco Express Forwarding Functional Overview

CEF 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 CEF operation are the FIB and Adjacency tables.

CEF uses adjacency tables to prepend Layer 2 addressing information. The 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. CEF discovers and solves adjacencies and populates the adjacency tables.

CISCO-CEF-MIB Benefits

Command-line interface (CLI) **show** commands are available to obtain CEF operational information. Managing CEF using the CLI can be a time consuming task. The increasing capacity of Cisco routers makes parsing through the **show** commands output to obtain the needed CEF operational parameters more and more difficult.

In Cisco IOS Release 12.2(31)SB and later releases, the CISCO-CEF-MIB allows you to manage and monitor the CEF operation using SNMP. In addition, you can configure SNMP to notify you if CEF encounters errors.

With the CISCO-CEF-MIB introduced with the Cisco Express Forwarding—SNMP CEF-MIB Support feature, you can access in real time operational information stored in the FIB and adjacency tables, switching statistics, information on resource failures, and configure parameters related to CEF 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.

CEF is available in all Cisco routers. However, CISCO-CEF-MIB support of CEF management is dependent on the new infrastructure introduced in Cisco IOS Release 12.2(22)S.

The implementation of the CISCO-CEF-MIB in Cisco IOS Release 12.2(31)SB2 manages CEF instances running on the Route Processor (RP). Information about CEF running on the line cards is available to the RP about CEF peers only.

The CISCO-CEF-MIB supports configuration and monitoring for both IP Versions, IP Version 4 (IPv4) and Version 6 (IPv6).

CEF 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:

- CEF administrative and operational states as displayed in the output of the **show ip cef summary** command

- Notifications for CEF events: CEF state changes, CEF failures (with a predefined reason), and Route Processor (RP) and line card inconsistencies.

- CEF-related parameters for the associated interface as displayed by the **show cef interface** command)

- Line card CEF states and line card CEF FIB states in the Linecard table as displayed by the **show cef linecard** command

- CEF statistics: switching statistics, punt and punt-to-host counters as displayed by the **show ip cef switching stats** command, and per-prefix counters and nonrecursive counters

- Notification for both IPv4 and IPv6, when CEF is switched between disable and enable and between CEF and distributed CEF

The SNMP CISCO-CEF-MIB provides managed objects that enable a network administrator to configure the following:

- CEF and dCEF administration status:

- CEF accounting-related parameters

- CEF load sharing-related parameters

- Traffic-related configuration parameters

CISCO-CEF-MIB Object Groups and Related Tables

The SNMP CISCO-CEF-MIB allows the configuration and management of CEF related objects. 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 CEF object groups. These tables provide information about prefixes, forwarding paths, adjacencies, output chain elements (OCEs), prefix-based statistics, information about CEF configuration, consistency checkers, switching statistics, and line card-specific managed objects.

The CISCO-CEF-MIB also defines CEF 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.

Brief Description of the Tables in the CISCO-CEF-MIB

Following is a list and a brief description of the tables provided by the CISCO-CEF-MIB:

- The CEF FIB Summary table (cefFIBSummaryTable) contains the number of forwarding prefixes for both IPv4 and IPv6 protocols; 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 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 CEF: administration and operational status, accounting-related configuration parameters, load-sharing algorithms and IDs, and traffic statistics parameters.

- CEF Interface table (cefIntTable) contains the interface specific CEF parameter: 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 CEF information related to peers on a managed line card: line card operational state and the number of time 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 Stats 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 parameter 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 "CEF Configuration and Monitoring Operations Available Through the CISCO-CEF-MIB" section on page 6 for information about the specific objects available through the CISCO-CEF-MIB tables.

Figure 1 shows the contents of the CISCO-CEF-MIB core tables and the relationships of the tables to one another.

Figure 1 **CISCO-CEF-MIB Main Tables, Table Contents, and Relationships**
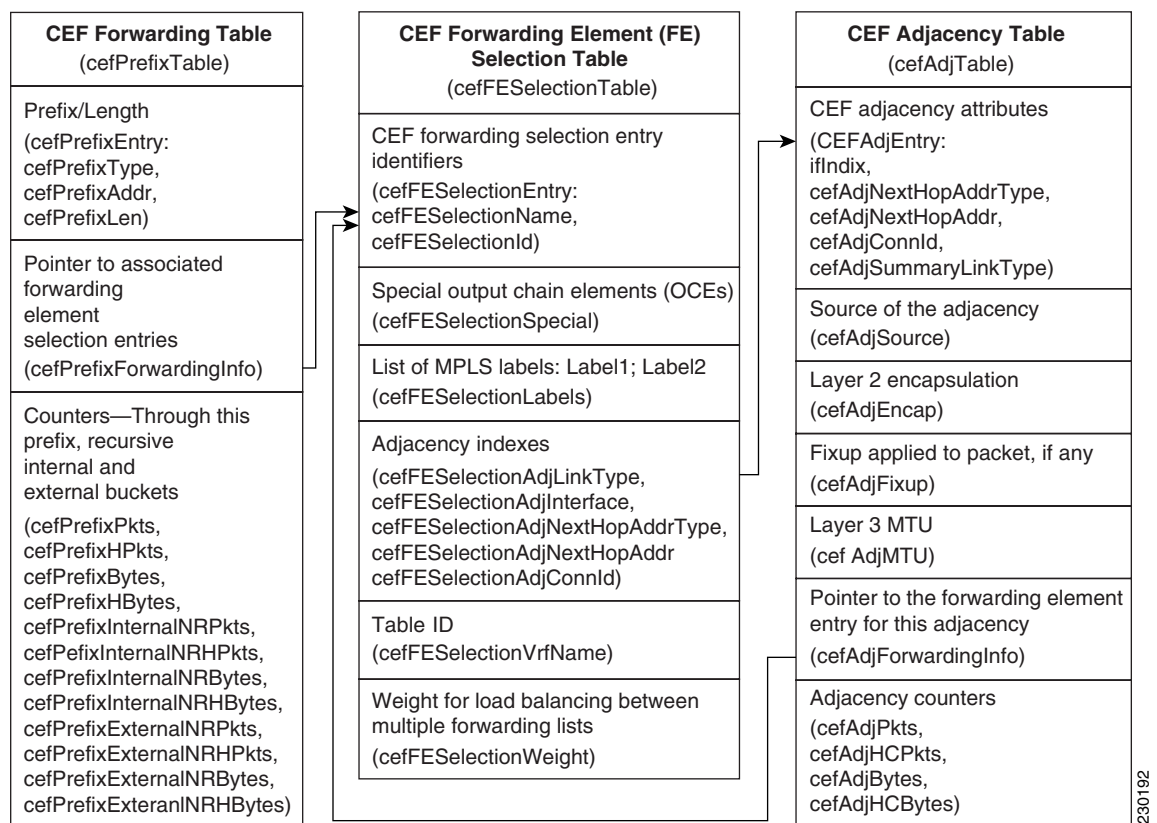
CEF Configuration and Monitoring Operations Available Through the CISCO-CEF-MIB

You can use SNMP **get** and **set** commands to configure and monitor CEF operations that are available through the CISCO-CEF-MIB tables. This section describes the configuration and monitoring operations for each table.

Table 1 lists the CEF monitoring operations and associated MIB objects provided by the CEF FIB Summary table (cefFIBSummaryTable).

Table 1   *CEF FIB Summary Table—CEF Operation and Associated MIB Object*

CEF Operation	Description
Gets the number of forwarding prefixes for IPv4 and IPv6	cefFIBSummaryFwdPrefixes

Table 2 lists the CEF monitoring operations and associated MIB objects provided by the CEF Forwarding table (cefPrefixTable).

Table 2   *CEF Forwarding Table—CEF Operations and Associated MIB Objects*

CEF Operation	MIB Object
Gets the forwarding information for the entry	cefPrefixForwardingInfo
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 non-recursive bytes forwarded by the prefix	cefPrefixInternalNRBytes
Gets the number of internal non-recursive bytes forwarded by the prefix in a 64-bit value	cefPrefixInternalNRHCBytes
Gets the number of external non-recursive packets forwarded by the prefix	cefPrefixExternalNRPkts
Gets the number of external non-recursive packets forwarded by the prefix in a 64-bit value	cefPrefixExternalNRHCPkts
Gets the number of external non-recursive bytes forwarded by the prefix	cefPrefixExternalNRBytes
Gets the number of external non-recursive bytes forwarded by the prefix in 64-bit value	cefPrefixExternalNRHCBytes

Table 3 lists the CEF monitoring operations and associated MIB objects provided by the CEF Longest Match Prefix table (cefLMPrefixTable).

Table 3   *CEF Longest Match Prefix Table—CEF Operations and Associated MIB Objects*

CEF 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

Table 3   CEF Longest Match Prefix Table—CEF Operations and Associated MIB Objects

CEF Operation	MIB Object
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

Table 4 lists the CEF monitoring operations and associated MIB objects provided by the CEF Path table (cefPathTable).

Table 4   CEF Path Table—CEF Operations and Associated MIB Objects

CEF Operation	MIB Object
Gets the type of CEF path for a prefix	cefPathType
Gets interface associated with this CEF path	cefPathInterface
Gets the next-hop address for the CEF path	cefPathNextHopAddr
Gets the recursive Virtual Private Network (VPN) routing and forwarding (VRF) instance name associated with this path	cefPathRecurseVrfName

Table 5 lists the CEF monitoring operations and associated MIB objects provided by the CEF Adjacency Summary table (cefAdjSummaryTable).

Table 5   CEF Adjacency Summary Table—CEF Operations and Associated MIB Objects

CEF 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

Table 6 lists the CEF monitoring operations and associated MIB objects provided by the Adjacency table (cefAdjTable).

Table 6   CEF Adjacency Table—CEF Operations and Associated MIB Objects

CEF Operation	MIB Object
Gets the adjacency source	cefAdjSource
Gets the adjacency Layer 2 encapsulation	cefAdjEncap
Gets the adjacency fix-up	cefAdjFixup
Gets the Layer 3 maximum transmission unit (MTU) for the adjacency	cefAdjMTU

Table 6 *CEF Adjacency Table—CEF Operations and Associated MIB Objects (continued)*

CEF Operation	MIB Object
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

Table 7 lists the CEF monitoring operations and associated MIB objects provided by the CEF Forwarding Element Selection table (cefFESelectionTable).

Table 7 *CEF Forwarding Element Selection Table—CEF Operations and Associated MIB Objects*

CEF Operation	MIB Object
Gets any special processing for a forwarding element	cefFESelectionSpecial
Gets the Multiprotocol Label Switching (MPLS) labels for forwarding element	cefFESelectionLabels
Gets the adjancency type for the forwarding element	cefFESelectionAdjLinkType
Gets the interface for the adjacency for the forwarding element	cefFESelectionAdjInterface
Gets the next-hop address type for the adjacency for the forwarding element	cefFESelectionAdjNextHopAddrType
Gets the next-hop address for the adjacency for the forwarding element	cefFESelectionAdjNextHopAddr
Gets the connection ID for the adjacency for the forwarding element	cefFESelectionAdjConnId
Gets the VRF name for the lookup for the forwarding element	cefFESelectionVrfName
Gets the weighting for load balancing for the forwarding element	cefFESelectionWeight

Table 8 lists the CEF configuration and monitoring operations and associated MIB objects provided by the CEF Cfg table (cefCfgTable).

Table 8 *CEF Cfg Table—CEF Operations and Associate MIB Objects*

CEF Operation	MIB Objects
Enables or disables a CEF instance	cefCfgAdminState
Queries a CEF operational instance	cefCfgOperState
Enables or disables a dCEF instance	cefCfgDistributionAdminState
Queries a dCEF operational instance	cefCfgDistributionOperState

Table 8   CEF Cfg Table—CEF Operations and Associate MIB Objects (continued)

CEF Operation	MIB Objects
Gets or sets CEF network accounting options	cefCfgAccountingMap • nonRecursive (0) • perPrefix (1) • prefixLength (2)
Gets or sets CEF load sharing algorithm options	cefCfgLoadSharingAlgorithm • none (1) - Load sharing is disabled. • original (2) • tunnel (3) • universal (4)
Gets or sets a load sharing ID	cefCfgLoadSharingID
Gets or sets a traffic interval timer for CEF traffic statistics	cefCfgTrafficStatsLoadInterval
Gets or sets a frequency timer for the line card to send traffic statistics to the RP	cefCfgTrafficStatsUpdateRate

Table 9 lists the CEF monitoring operations and associated MIB objects provided by the CEF Resource table (cefResourceTable).

Table 9   CEF Resource Table—CEF Operations and Associate MIB Objects

CEF Operation	MIB Object
Gets the memory status of process memory pool for CEF	cefResourceMemoryUsed
Gets the reason for the CEF resource failure notification	cefResourceFailureReason

Table 10 lists the CEF configuration and monitoring operations and associated MIB objects provided by the CEF Interface table (cefIntTable).

Table 10   CEF Interface Table—CEF Operations and Associate MIB Objects

CEF Operation	MIB Objects
Gets or sets the CEF switching state of the interface	cefIntSwitchingState • cefEnabled (1) • distCefEnabled (2) • cefDisabled (3)
Gets or sets the kind of CEF Load sharing on the interface	cefIntLoadSharing • perPacket (1) • perDestination (2)
Gets or sets CEF non-recursive accounting on the interface	cefIntNonrecursiveAccouting • internal (1) • external (2)

Table 11 lists the CEF monitoring operations and associated MIB objects provided by the CEF Peer table (or Linecard table) (cefPeerTable).

Table 11   CEF Peer Table—CEF Operations and Associate MIB Objects

CEF Operation	MIB Objects
Gets the CEF operational instance of the peer entity	cefPeerOperState
Gets the number of times the session with the Peer resets	cefPeerNumberOfResets

Table 12 lists the CEF monitoring operation and associated MIB object provided by the CEF Peer FIB table (cefPeerFIBTable).

Table 12   CEF Peer FIB Table—CEF Operation and Associate MIB Object

CEF Operation	MIB Objects
Gets the current CEF FIB operation state of the peer entity	cefPeerFIBOperState

Table 13 lists the CEF monitoring operations and associated MIB objects provided by the CEF Prefix length Statistics table (cefStatsPrefixTable).

Table 13   CEF Prefix Length Statistics Table—CEF Operations and Associated MIB Objects

CEF 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

Table 14 lists the CEF monitoring operations and associated MIB objects provided by the CEF Switching Statistics table (cefSwitchingStatsTable).

Table 14   *CEF Switching Statistics Table—CEF Operations and Associate MIB Objects*

CEF Operation	MIB Objects
Gets the switching path of a CEF instance	cefSwitchingPath
Gets the number of packets dropped by a CEF instance	cefSwitchingDrop
Gets the number of packets dropped by a CEF 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

Table 15 lists the CEF configuration and monitoring operations and associated MIB objects provided by the CEF IP Prefix Consistency Checker group (cefCCGlobalTable).

Table 15   *CEF IP Prefix Consistency Checker Group—CEF Operations and Associate MIB Objects*

CEF 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 re-enable auto-repair after auto-repair runs	cefCCGlobalAutoRepairHoldDown
Enables or disables error message generation for an inconsistency	cefCCGlobalErrorMsgEnabled

Table 16 lists the CEF configuration and monitoring operations and associated MIB objects provided by the CEF Consistency Checker Type table (cefCCTypeTable).

Table 16   *CEF Consistency Checker Type Table—CEF Operations and Associate MIB Objects*

CEF Operation	MIB Objects
Enables or disables the passive consistency checker	cefCCEnabled
Get 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 CEF FIB	cefCCQueriesSent
Gets the number of prefix consistency queries ignored by the consistent checker	cefCCQueriesIgnored

Table 16   CEF Consistency Checker Type Table—CEF Operations and Associate MIB Objects

CEF Operation	MIB Objects
Gets the number of prefix consistent queries iterated back to the database	cefCCQueriesIterated
Gets the number of prefix consistent queries processed	cefCCQueriesChecked

Table 17 lists the CEF configuration and monitoring operations and associated MIB objects provided by the CEF Inconsistency Record table (cefInconsistencyRecordTable).

Table 17   CEF Inconsistency Record Table—CEF Operations and Associate MIB Objects

CEF 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 • missing (1) • checksumErr (2) • unknown (3)
Global Objects for CEF Inconsistency	
Gets the value of the system uptime at the time an inconsistency was detected	entLastInconsistencyDetectTime
Sets an object to restart all active consistency checkers	cefInconsistencyReset
Gets the status of the inconsistency reset request	cefInconsistencyResetStatus

CISCO-CEF-MIB Notifications

Table 18 lists the CEF operations associated with the CISCO-CEF-MIB objects that enable the sending of CEF notifications.

Table 18   CEF Notifications—CEF Operations and CISCO-CEF-MIB Objects that Enable Them

CEF Operation	MIB Object
Enables the sending of a notification on the detection of a CEF resource failure.	cefResourceFailureNotifEnable
Enables the sending of a notification on the detection of a CEF peer state change.	cefPeerStateChangeNotifEnable
Enables the sending of a notification on the detection of a CEF FIB peer state change.	cefPeerFIBStateChangeNotifEnable

Table 18 CEF Notifications—CEF Operations and CISCO-CEF-MIB Objects that Enable Them

CEF Operation	MIB Object
Sets the period of time between the sending of notification events.	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. Table 19 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 19 Description of Notifications and Enabling Commands for the CEF-PROVISION-MIB Notifications

Notification	Generated for	Commands
CEF 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** MIB: **setany** *version ip-address community-string* **cefResourceFailureNotifEnable.0 -i 1**
CEF 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** MIB: **setany** *version ip-address community-string* **cefPeerStateChangeNotifEnable.0 -i 1**
CEF 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** MIB: **setany** *version ip-address community-string* **cefPeerFIBStateChangeNotifEnable.0 -i 1**
CEF inconsistency detection notification	An inconsistencies detected by the consistency checkers	CLI: **snmp-server enable traps cef inconsistency** MIB: **setany** *version ip-address community-string* **cefInconsistencyNotifEnable.0 -i 1**

How to Configure Cisco Express Forwarding—SNMP CEF-MIB Support

Perform the following tasks to configure Cisco Express Forwarding—SNMP CEF-MIB Support.

- Configuring the Router to Use SNMP, page 15 (required)
- Configuring an SNMP Host to Receive CISCO-CEF-MIB Notifications, page 17 (required)
- Configuring SNMP Notifications for Cisco Express Forwarding Events, page 20 (required)
- Configuring the Throttling Interval for CISCO-CEF-MIB Inconsistency Notification, page 24 (optional)

Configuring the Router to Use SNMP

Perform the following task to configure the 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`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	`snmp-server community` *string* [`view` *view-name*] [`ro` | `rw`] [`ipv6 nacl`] [*access-list-number*] **Example:** `Router(config)# snmp-server community public ro`	Sets up the community access string to permit access to SNMP. • 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. • 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. • The **ro** keyword specifies read-only access. Authorized management stations can only retrieve MIB objects. • The **rw** keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects. • The **ipv6 nacl** keywords specify the IPv6 named access list. • 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 allowed access to the SNMP agent. 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. **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 wish 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 this step.

	Command or Action	Purpose

Step 4	`snmp-server community` *string2* `rw`
	
	Example:
	`Router(config)# snmp-server community private`
	`rw`
		Sets up the community access string to permit access to SNMP.
		
		• 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.
		
		• The **rw** keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects.
		
		This example allows MIB objects to be retrieved and set because a string is specified with read-write access.
		
		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 wish to only 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	`end`
	
	Example:
	`Router(config)# end`
		Exits to privileged EXEC mode.

Configuring an SNMP Host to Receive CISCO-CEF-MIB Notifications

Perform the following task to configure an SNMP host to receive CISCO-CEF-MIBnotifications. Notifications provide information to assist you in the monitoring and managing of CEF 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`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`snmp-server community` *string* [**ro** | **rw**] **Example:** `Router(config)# snmp-server community public ro`	Sets up the community access string to permit access to SNMP. • 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. • The **ro** keyword specifies read-only access. Authorized management stations can only retrieve MIB objects. • The **rw** keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects.
Step 4	`snmp-server community` *string2* **rw** **Example:** `Router(config)# snmp-server community private rw`	Sets up the community access string to permit access to SNMP. • 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. • The **rw** keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects. This example allows MIB objects to be retrieved and set because a string is specified with read-write access. **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 wish to only 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).

	Command or Action	Purpose

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`
	
	Example:
	`Router(config)# snmp-server host 10.56.125.47 informs version 2c public cef`
		Specifies the recipient of an SNMP notification operation.
		
		• The *ip-address* argument is the IP address or IPv6 address of the SNMP notification host.
		
		The SNMP notification host is typically a network management station (NMS or SNMP manager). This host is the recipient of the SNMP traps or informs.
		
		• The **vrf** *vrf-name* keyword and argument specify that the specified VRF be used to send SNMP notifications.
		
		• The **traps** keyword specifies that notifications should be sent as traps. This is the default.
		
		• The **informs** keyword specifies that notifications should be sent as informs.
		
		• The version keyword specifies the version of the SNMP used to send the traps. The default is 1.
		
		If you use the **version** keyword, one of the following keywords must be specified:
		
		– **1**—SNMPv1. This option is not available with informs.
		
		– **2c**—SNMPv2c.
		
		– **3**—SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**.
		
		• One of the following three optional security level keywords can follow the **version 3** keywords:
		
		– **auth**—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.
		
		– **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.
		
		– **priv**—Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
		
		• The *community-string* argument specifies that a password-like community string be sent with the notification operation.
		
		• The **udp-port** *port* keyword and argument specify that SNMP notifications or informs are to be sent to the UDP port number of the NMS host. The default is 162.
		
		• 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.

	Command or Action	Purpose

Step 6	`end`
	
	Example:
	`Router(config)# end`
		Exits to privileged EXEC mode.

What to Do Next

After you configure an SNMP host to receive the CISCO-CEF-MIB notifications, you can configure the notifications that you want to receive. See the "Configuring SNMP Notifications for Cisco Express Forwarding Events" section on page 20.

Configuring SNMP Notifications for Cisco Express Forwarding Events

Perform the following task to configure SNMP notifications for CEF events. You can complete the task through the use of CLI commands or SNMP commands.

Prerequisites

You need to configure an NMS or SNMP agent to receive the SNMPCISCO-CEF-MIB notification, see the "Configuring an SNMP Host to Receive CISCO-CEF-MIB Notifications" section on page 17

SUMMARY STEPS

Router CLI Commands

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**

SNMP Commands

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: Router CLI Commands

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`snmp-server enable traps cef`
	`[`**`peer-state-change`**`] [`**`resource-failure`**`]`
	`[`**`inconsistency`**`] [`**`peer-fib-state-change`**`]`
	
	Example:
	`Router(config)# snmp-server enable traps cef`
	`resource-failure`
		Enables Cisco Express Forwarding support of SNMP notifications on an NMS.
		
		• The **peer-state change** keyword enables the sending of CISCO-CEF-MIB SNMP notifications for changes in the operational state of CEF peers.
		
		• The **resource-failure** keyword enables the sending of CISCO-CEF-MIB SNMP notifications for resource failures that affect CEF operations.
		
		• 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.
		
		You can set the throttling interval for sending inconsistency notifications, see the "Configuring the Throttling Interval for CISCO-CEF-MIB Inconsistency Notification" section on page 24.
		
		• The **peer-fib-state-change** keyword enables the sending of CISCO-CEF-MIB SNMP notifications for changes in the operational state of the CEF peer FIB.

	Command or Action	Purpose

Step 4	**snmp-server host** *ip-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* **cef**
	
	Example:
	Router(config)# snmp-server host 10.56.125.47 informs version 2c public cef
		Specifies the recipient of an SNMP notification operation.
		
		• The *ip-address* argument is the IP address or IPv6 address of the SNMP notification host.
		
		The SNMP notification host is typically a network management station (NMS or SNMP manager). This host is the recipient of the SNMP traps or informs.
		
		• The **traps** keyword specifies that notifications should be sent as traps. This is the default.
		
		• The **informs** keyword specifies that notifications should be sent as informs.
		
		• The version keyword specifies the version of the SNMP used to send the traps. The default is 1.
		
		If you use the **version** keyword, one of the following keywords must be specified:
		
		  – **1**—SNMPv1. This option is not available with informs.
		  – **2c**—SNMPv2C.
		  – **3**—SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is **noauth**.
		
		• One of the following three optional security level keywords can follow the **version 3** keywords:
		
		  – **auth**—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.
		  – **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.
		  – **priv**—Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
		
		• The *community-string* argument specifies that a password-like community string be sent with the notification operation.
		
		• 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** **Example:** Router(config)# end	Exits to privileged EXEC mode.

DETAILED STEPS: SNMP Commands

	Command or Action	Purpose

Step 1	**setany** *version ip-address community-string* **cefPeerStateChangeNotifEnable.0 -i** *TruthValue*
	
	Example:
	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.
		
		• The *version* argument specifies the version of SNMP that is used. Options are
		   – **-v1**—SNMPv1
		   – **-v2c**—SNMPv2C
		   – **-v3**—SNMPv3
		• The *ip-address* argument is the IP address or IPv6 address of the SNMP notification host.
		
		The SNMP notification host is typically a network management station (NMS or SNMP manager). This host is the recipient of the SNMP traps or informs.
		
		• The *community-string* argument specifies that a password-like community string be sent with the notification operation.
		• The **-i** keywords indicate that the variable that follows is an integer.
		• Values for the *TruthValue* argument are:
		   – 1—enable sending of the notification
		   – 2—disable sending of the notification
		
		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* **Example:** 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 CEF peer FIB. • See Step 1 for a description of the command arguments and keywords.
Step 3	**setany** *version ip-address* community-string **cefResourceFailureNotifEnable.0 -i** *TruthValue* **Example:** 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. • See Step 1 for a description of the command arguments and keywords.
Step 4	**setany** *version ip-address community-string* **cefInconsistencyNotifEnable.0 -i** *TruthValue* **Example:** 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 CEF FIB on the RP and to the CEF FIB on the line cards. • See Step 1 for a description of the command arguments and keywords.

Configuring the Throttling Interval for CISCO-CEF-MIB Inconsistency Notification

Perform the following task to configure the throttling interval for CISCO-CEF-MIB inconsistency notifications.

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 result, due to the asynchronous nature of the distribution mechanism for these databases. The throttling interval allows fleeting inconsistencies to resolve themselves before sending an inconsistence notification.

SUMMARY STEPS

Router CLI Commands

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps cef inconsistency**
4. **snmp mib cef throttling-interval** *seconds*
5. **end**

SNMP Commands

1. **setany** *version ip-address community-string* **cefNotifThrottlingInterval.0 -i** *seconds*

DETAILED STEPS:

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`snmp-server enable traps cef inconsistency`
	
	Example:
	`Router(config)# snmp-server enable traps cef inconsistency`
		Enables the sending of CISCO-CEF-MIB SNMP notifications for inconsistencies in Cisco Express Forwarding.

	Command or Action	**Purpose**
Step 4	`snmp mib cef throttling-interval` *seconds* **Example:** `Router(config)# snmp mib cef throttling-interval 2500`	Sets the throttling interval for the CISCO-CEF-MIB inconsistency notifications. • 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. The valid value is from 1 to 3600 seconds. A value of 0 disables throttle control.

Step 5	`end`
	
	Example:
	`Router(config)# end`
		Exits to privileged EXEC mode.

DETAILED STEPS: SNMP Commands

	Command or Action	**Purpose**

Step 1	`setany` *version ip-address community-string* `cefNotifThrottlingInterval.0 -i` *seconds*
	
	Example:
	`workstation% setany -v2c 10.56.125.47 public cefNotifThrottlingInterval.0 -1 3600`
		Sets the throttling interval for the CISCO-CEF-MIB inconsistency notifications.
		
		• The *version* argument specifies the version of SNMP that is used. Options are
		
		   – **-v1**—SNMPv1
		
		   – **-v2c**—SNMPv2C
		
		   – **-v3**—SNMPv3
		
		• The *ip-address* argument is the IP address or IPv6 address of the SNMP notification host.
		
		The SNMP notification host is typically a network management station (NMS or SNMP manager). This host is the recipient of the SNMP traps or informs.
		
		• The *community-string* argument specifies that a password-like community string be sent with the notification operation.
		
		• The **-i** keywords indicate that the variable that follows is an integer.
		
		• 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. The valid value is from 1 to 3600 seconds. A value of 0 disables throttle control.

Configuration Examples for Cisco Express Forwarding—SNMP CEF-MIB Support

This section contains the following configuration examples for the Cisco Express Forwarding—SNMP CEF-MIB Support feature:

Configuring an SNMP Host to Receive CISCO-CEF-MIB Notifications: Example

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.

Configuring SNMP Notifications for Cisco Express Forwarding Events: Example

This section contains examples for configuring SNMP notifications for CEF events using the CLI and using SNMP commands.

Configuring SNMP Notifications for Cisco Express Forwarding Events Using the CLI: Example

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 CEF peer states and peer FIB states, for CEF resource failures, and for inconsistencies in CEF 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: Example

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 CEF peer states and peer FIB states, for CEF resource failures, and for inconsistencies in CEF 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
```

Configuring the Throttling Interval for CISCO-CEF-MIB Inconsistency Notifications: Example

This example shows the configuration of a throttling interval for the sending of CEF 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: Example

This example shows the addition of a throttling interval of 1000 seconds for the sending of CEF 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: Example

This example shows the addition of a throttling interval of 1000 seconds for the sending of CEF inconsistency notifications to the SNMP host using an SNMP command:

```
setany -v2c 10.56.125.47 public cefNotifThrottlingInterval.0 -1 1000
```

Additional References

The following sections provide references related to the Cisco Express Forwarding—SNMP CEF-MIB Support feature.

Related Documents

Related Topic	Document Title
Commands for configuring and managing Cisco Express Forwarding	*Cisco IOS IP Switching Services Command Reference*
Overview of Cisco Express Forwarding	"Cisco Express Forwarding Overview"
Tasks for configuring Cisco Express Forwarding	"Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks"

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: 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 Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **snmp mib cef throttling-interval**
- **snmp-server enable traps cef**
- **snmp-server host**

snmp mib cef throttling-interval

To set the throttling interval for the CEF-MIB inconsistency notifications, use the **snmp mib cef throttling-interval** command in global configuration mode. To remove the throttling interval, use the **no** form of this command.

> **snmp mib cef throttling-interval** *seconds*

> **no snmp mib cef throttling-interval** *seconds*

Syntax Description

seconds	The time to allow before an inconsistency notification is sent during the process of updating forwarding information from the Routing Information Base (RIB) to the Route Processor (RP) and the line card databases. The valid value is from 0 to 3600 seconds.

Command Default Throttling is disabled by default (throttling interval is set to 0 seconds).

Command Modes Global configuration

Command History

Release	Modification
12.2(31)SB	This command was introduced.

Usage Guidelines Use this command in conjunction with the **snmp-server enable traps cef inconsistency** command to set the time elapsed between the occurrence of a Cisco Express Forwarding database inconsistencies and the time when you want to receive an inconsistency notification.

If you set the throttling interval to 0 seconds, throttling is disabled.

Examples The following example shows how to set the throttling interval for CEF-MIB inconsistency notification to 300 seconds:

```
configure terminal
!
snmp-server enable traps cef inconsistency
snmp mib cef throttling-interval 300
```

Related Commands

Command	Description
snmp-server enable traps cef	Enables CEF-MIB notifications that correspond to Cisco Express Forwarding events.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps cef

To enable Cisco Express Forwarding (CEF) support of Simple Network Management Protocol (SNMP) notifications on a network management system (NMS), use the **snmp-server enable traps cef** command in global configuration mode. To disable Cisco Express Forwarding support of SNMP notifications, use the **no** form of this command.

> **snmp-server enable traps cef** [**peer-state-change**] [**resource-failure**] [**inconsistency**] [**peer-fib-state-change**]

> **no snmp-server enable traps cef** [**peer-state-change**] [**resource-failure**] [**inconsistency**] [**peer-fib-state-change**]

Syntax Description

peer-state-change	Enables the sending of CEF-MIB SNMP notifications for changes in the operational state of CEF peers.
resource-failure	Enables the sending of CEF-MIB SNMP notifications for resource failures that affect Cisco CEF operations.
inconsistency	Enables the sending of CEF-MIB SNMP notifications for inconsistencies that occur when routing information is updated from the Routing Information Base (RIB) to the CEF Forwarding Information Base (FIB) on the Route Processor (RP) and to the CEF FIB on the line cards.
peer-fib-state-change	Enables the sending of CEF-MIB SNMP notifications for changes in the operational state of the CEF peer FIB.

Command Default   All CEF-MIB notifications are disabled by default.

Command Modes   Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines   You can use this command to enable CEF-MIB SNMP notifications that correspond to specific Cisco Express Forwarding events. To send the notifications to an NMS or host system, you need to configure the **snmp-server host** command with the **cef** keyword.

You can enable all CEF-MIB SNMP notifications if you enter the **snmp-server enable traps cef** command without entering an optional keyword.

Examples The following example shows how to enable the router to send CEF peer state changes and forwarding inconsistencies as informs to the NMS with IP address 10.56.125.47 and to use the community string defined as public:

```
configure terminal
!
snmp-server enable traps cef peer-state-change inconsistency
snmp-server host 10.56.125.47 informs version 2c public
```

Related Commands

Command	Description
snmp-server community	Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

> **snmp-server host** {*hostname | ip-address*} [**vrf** *vrf-name*] [**traps | informs**] [**version** {**1 | 2c | 3** [**auth | noauth | priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

> **no snmp-server host** {*hostname | ip-address*} [**vrf** *vrf-name*] [**traps | informs**] [**version** {**1 | 2c | 3** [**auth | noauth | priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

Syntax Description		
*hostname	ip-address*	Name, IP address, or IPv6 address of the SNMP notification host. The *ip-address* can be an IP or IPv6 address.	
	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.	
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications.	
vrf-name	(Optional) VPN VRF instance used to send SNMP notifications.	
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.	
informs	(Optional) Specifies that notifications should be sent as informs.	
version	(Optional) Version of the SNMP used to send the traps. The default is 1.	
	If you use the **version** keyword, one of the following keywords must be specified:	
	• **1**—SNMPv1. This option is not available with informs.	
	• **2c**—SNMPv2C.	
	• **3**—SNMPv3. The most secure model because it allows packet encryption with the **priv** keyword. The default is noauth.	
	One of the following three optional security level keywords can follow the **3** keyword:	
	– **auth**—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.	
	– **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.	
	– **priv**—Enables Data Encryption Standard (DES) packet encryption (also called "privacy").	
community-string	Password-like community string is sent with the notification operation.	
	Note You can set this string using the **snmp-server host** command by itself, but Cisco recommends that you define the string using the **snmp-server community** command prior to using the **snmp-server host** command.	
	Note The sign (@) is used for delimiting the context information.	

udp-port	(Optional) Specifies that SNMP notifications or informs are to be sent to an NMS host.
port	(Optional) UDP port number of the NMS host. The default is 162.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of the following keywords:

- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **calltracker**—Sends Call Tracker call-start/call-end notifications.
- **cef** — Sends Cisco Express Forwarding-related notifications.
- **config**—Sends configuration change notifications.
- **cpu**—Sends CPU-related notifications.
- **director**—Sends DistributedDirector-related notifications.
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **eigrp**—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.
- **entity**—Sends Entity MIB modification notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **flash**—Sends flash media insertion and removal notifications.
- **frame-relay**—Sends Frame Relay notifications.
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
- **iplocalpool**—Sends IP local pool notifications.
- **ipmobile**—Sends Mobile IP notifications.
- **ipsec**—Sends IP Security (IPsec) notifications.
- **isdn**—Sends ISDN notifications.
- **l2tun-pseudowire-status**—Sends pseudowire state change notifications.
- **l2tun-session**—Sends Layer 2 tunneling session notifications.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **memory**—Sends memory pool and memory buffer pool notifications.
- **mpls-ldp**—Sends Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **repeater**—Sends standard repeater (hub) notifications.

- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC 2233 compliant link up/down notifications, you should use the **snmp server link trap** command.

- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stun**—Sends serial tunnel (STUN) notifications.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.
- **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **x25**—Sends X.25 event notifications.

Command Default   This command is disabled. No notifications are sent.

Command Modes   Global configuration

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	• The **version 3** [**auth** | **noauth** | **priv**] syntax was added as part of the SNMPv3 Support feature.
	• The **hsrp** notification-type keyword was added.
	• The **voice** notification-type keyword was added.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.

Release	Modification
12.2(2)T	• The **vrf** *vrf-name* keyword/argument combination was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	• The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
12.2(8)T	• The **mpls-traffic-eng** notification-type keyword was added. • The **director** notification-type keyword was added.
12.2(13)T	• The **srp** notification-type keyword was added. • The **mpls-ldp** notification-type keyword was added.
12.3(2)T	• The **flash** notification-type keyword was added. • The **l2tun-session** notification-type keyword was added.
12.3(4)T	• The **cpu** notification-type keyword was added. • The **memory** notification-type keyword was added. • The **ospf** notification-type keyword was added.
12.3(8)T	The **iplocalpool** notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The **vrrp** keyword was added.
12.3(14)T	• Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **eigrp** notification-type keyword was added.
Cisco IOS Release 12.0S	
12.0(17)ST	The **mpls-traffic-eng** notification-type keyword was integrated into Cisco IOS Release 12.0(17)ST.
12.0(21)ST	The **mpls-ldp** notification-type keyword was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	• All features in the Cisco IOS Release 12.0ST train were integrated into Cisco IOS Release 12.0(22)S. • The **mpls-vpn** notification-type keyword was added.
12.0(23)S	The **l2tun-session** notification-type keyword was added.
12.0(26)S	The **memory** notification-type keyword was added.
12.0(27)S	• Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the *hostname* argument. • The **vrf** *vrf-name* keyword argument pair was integrated into Cisco IOS Release 12.0(27)S to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	The **l2tun-pseudowire-status** notification-type keyword was added.
Release 12.2S	**Modification**
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

Release	Modification
12.2(25)S	• The **cpu** notification-type keyword was added.
	• The **memory** notification-type keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The **cef** notification-type keyword was added.

Usage Guidelines

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

> **Note** If the community-string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community-string) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, a SNMP entity that receives an inform request acknowledges the message with a SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter a **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled and others are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

A notification-type option's availability depends on the router type and Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a customer so data is stored using the VPN.

Regarding Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no intervening spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls-traffic-eng** (containing an intervening space and a hyphen).

This syntax difference is necessary to ensure that the command-line interface (CLI) interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 20 maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 20   Notification Keywords and Corresponding SNMP Enable Traps Commands

SNMP Enable Traps Command	SNMP Host Command Keyword
snmp-server enable traps l2tun session	**l2tun-session**
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng[1]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**

1. See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

Note   The sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN_ID (for example, public@100) where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a host specified named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 172.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to company.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host company.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 10.56.125.47 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 10.56.125.47 informs version 2c public cef
```

Related Commands

Command	Description
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP traps, which are compliant with RFC 2233.

Command	Description
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which a SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

Feature Information for Cisco Express Forwarding—SNMP CEF-MIB Support

Table 21 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 21 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software also support that feature.

Table 21 **Feature Information for Cisco Express Forwarding—SNMP CEF-MIB Support**

Feature Name	Releases	Feature Information
Cisco Express Forwarding—SNMP CEF-MIB Support	12.2(31)SB2	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 (CEF) operational data and to provide notification when CEF encounters specific configured events. This module describes how to use the CISCO-CEF-MIB to manage and monitor objects related to CEF operation. In 12.2(31)SB2, this feature was introduced on the Cisco 10000. The following sections provide information about this feature: • Cisco Express Forwarding Functional Overview, page 3 • CISCO-CEF-MIB Benefits, page 3 • CEF Information Managed by the CISCO-CEF-MIB, page 3 • CISCO-CEF-MIB Object Groups and Related Tables, page 4 • Brief Description of the Tables in the CISCO-CEF-MIB, page 5 • CEF Configuration and Monitoring Operations Available Through the CISCO-CEF-MIB, page 6 • CISCO-CEF-MIB Notifications, page 13 • Configuring the Router to Use SNMP, page 15 • Configuring an SNMP Host to Receive CISCO-CEF-MIB Notifications, page 17 • Configuring SNMP Notifications for Cisco Express Forwarding Events, page 20 • Configuring the Throttling Interval for CISCO-CEF-MIB Inconsistency Notification, page 24 The following commands were introduced or modified by this feature: **snmp mib cef throttling-interval**, **snmp-server enable traps cef**, and **snmp-server host**.

Glossary

informs—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 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 software IPC services allow line cards (LCs) and the central route processor (RP) in a distributed system, such as a Cisco 7500 series router, 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. *See also* trap.

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 communities—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 (notifications) 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. *See also* notification.

XDR—External Data Representation. Information elements inside Inter-Process Communication (IPC) messages in which Cisco Express Forwarding updates are encoded in distributed packet forwarding.

Note   See *Internetworking Terms and Acronyms* for terms not included in this glossary.

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

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

© 2006 Cisco Systems, Inc. All rights reserved.