IP Switching Configuration Guide, Cisco IOS Release 15.1M&T

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

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.

IP Switching Configuration Guide, Cisco IOS Release 15.1M&T
© 2010 Cisco Systems, Inc. All rights reserved.

About Cisco IOS Software Documentation

Last Updated: March 26, 2010

This document describes the objectives, audience, conventions, and organization used in Cisco IOS software documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section contains the following topics:

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the **^** symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, that is enclosed within braces or square brackets indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS software uses the following program code conventions:

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

Cisco IOS documentation uses the following conventions for reader alerts:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

Cisco IOS Documentation Set

The Cisco IOS documentation set consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the organization of the Cisco IOS documentation set and how to access various document types.

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.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books contain descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xi.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references contain commands for Cisco IOS software for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

http://www.cisco.com/go/techdocs

Table 1 Cisco IOS Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS AppleTalk Configuration Guide* • *Cisco IOS AppleTalk Command Reference*	AppleTalk protocol.
• *Cisco IOS Asynchronous Transfer Mode Configuration Guide* • *Cisco IOS Asynchronous Transfer Mode Command Reference*	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging Command Reference* • *Cisco IOS IBM Networking Command Reference*	Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
• *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide* • *Cisco IOS Broadband Access Aggregation and DSL Command Reference*	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Carrier Ethernet Configuration Guide* • *Cisco IOS Carrier Ethernet Command Reference*	Operations, Administration, and Maintenance (OAM); Ethernet connectivity fault management (CFM); ITU-T Y.1731 fault management functions; Ethernet Local Management Interface (ELMI); MAC address support on service instances, bridge domains, and pseudowire; IEEE 802.3ad Link Bundling; Link Aggregation Control Protocol (LACP) support for Ethernet and Gigabit Ethernet links and EtherChannel bundles; LACP support for stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF), and nonstop routing (NSR) on Gigabit EtherChannel bundles; and Link Layer Discovery Protocol (LLDP) and media endpoint discovery (MED).
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
• *Cisco IOS DECnet Configuration Guide* • *Cisco IOS DECnet Command Reference*	DECnet protocol.
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
• *Cisco IOS Flexible NetFlow Configuration Guide* • *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.
• *Cisco IOS High Availability Configuration Guide* • *Cisco IOS High Availability Command Reference*	A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
• *Cisco IOS Intelligent Services Gateway Configuration Guide* • *Cisco IOS Intelligent Services Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
• *Cisco IOS Interface and Hardware Component Configuration Guide* • *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
• *Cisco IOS IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS IP Application Services Configuration Guide* • *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
• *Cisco IOS IP Mobility Configuration Guide* • *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
• *Cisco IOS IP Multicast Configuration Guide* • *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
• *Cisco IOS IP Routing: BFD Configuration Guide*	Bidirectional forwarding detection (BFD).
• *Cisco IOS IP Routing: BGP Configuration Guide* • *Cisco IOS IP Routing: BGP Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
• *Cisco IOS IP Routing: EIGRP Configuration Guide* • *Cisco IOS IP Routing: EIGRP Command Reference*	Enhanced Interior Gateway Routing Protocol (EIGRP).
• *Cisco IOS IP Routing: ISIS Configuration Guide* • *Cisco IOS IP Routing: ISIS Command Reference*	Intermediate System-to-Intermediate System (IS-IS).
• *Cisco IOS IP Routing: ODR Configuration Guide* • *Cisco IOS IP Routing: ODR Command Reference*	On-Demand Routing (ODR).
• *Cisco IOS IP Routing: OSPF Configuration Guide* • *Cisco IOS IP Routing: OSPF Command Reference*	Open Shortest Path First (OSPF).
• *Cisco IOS IP Routing: Protocol-Independent Configuration Guide* • *Cisco IOS IP Routing: Protocol-Independent Command Reference*	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
• *Cisco IOS IP Routing: RIP Configuration Guide* • *Cisco IOS IP Routing: RIP Command Reference*	Routing Information Protocol (RIP).
• *Cisco IOS IP SLAs Configuration Guide* • *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
• *Cisco IOS IP Switching Configuration Guide* • *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
• *Cisco IOS IPv6 Configuration Guide* • *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document.
• *Cisco IOS ISO CLNS Configuration Guide* • *Cisco IOS ISO CLNS Command Reference*	ISO Connectionless Network Service (CLNS).

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS LAN Switching Configuration Guide* • *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
• *Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide* • *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
• *Cisco IOS Mobile Wireless Home Agent Configuration Guide* • *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
• *Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide* • *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
• *Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide* • *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.
• *Cisco IOS Multiprotocol Label Switching Configuration Guide* • *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.
• *Cisco IOS Multi-Topology Routing Configuration Guide* • *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
• *Cisco IOS NetFlow Configuration Guide* • *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, and export features.
• *Cisco IOS Network Management Configuration Guide* • *Cisco IOS Network Management Command Reference*	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration).
• *Cisco IOS Novell IPX Configuration Guide* • *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring and automatic route optimization and load distribution for multiple connections between networks.
• *Cisco IOS Performance Routing Configuration Guide*	Performance Routing (PfR) provides additional intelligence to classic routing technologies to track the performance of, or verify the quality of, a path between two devices over a WAN infrastructure in order to determine the best egress or ingress path for application traffic.
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
• *Cisco IOS Security Command Reference*	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS+; terminal access security; and traffic filters.
• *Cisco IOS Security Configuration Guide: Securing the Data Plane*	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• *Cisco IOS Security Configuration Guide: Securing the Control Plane*	Control Plane Policing, Neighborhood Router Authentication.
• *Cisco IOS Security Configuration Guide: Securing User Services*	AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.
• *Cisco IOS Security Configuration Guide: Secure Connectivity*	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.
• *Cisco IOS Service Advertisement Framework Configuration Guide* • *Cisco IOS Service Advertisement Framework Command Reference*	Cisco Service Advertisement Framework.
• *Cisco IOS Service Selection Gateway Configuration Guide* • *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Software Activation Configuration Guide* • *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
• *Cisco IOS Software Modularity Installation and Configuration Guide* • *Cisco IOS Software Modularity Command Reference*	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes, and patches.
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
• *Cisco IOS Virtual Switch Command Reference*	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). **Note** For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
• *Cisco IOS VPDN Configuration Guide* • *Cisco IOS VPDN Command Reference*	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy; L2TP extended failover; L2TP security VPDN; multihop by Dialed Number Identification Service (DNIS); timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F); RADIUS Attribute 82 (tunnel assignment ID); shell-based authentication of VPDN users; tunnel authentication via RADIUS on tunnel terminator.
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.
• *Cisco IOS Wireless LAN Configuration Guide* • *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title or Resource	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS System Message Guide	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or system software.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator.
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is released monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

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.

© 2008–2010 Cisco Systems, Inc. All rights reserved.

Using the Command-Line Interface in Cisco IOS Software

Last Updated: February 24, 2010

This document provides basic information about the command-line interface (CLI) in Cisco IOS software and how you can use some of the CLI features. This document contains the following sections:

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS Software Documentation" document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product/Technologies Support area of Cisco.com at http://www.cisco.com/go/techdocs.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

Note The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 1 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a Ctrl-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on Cisco ASR 1000 series routers)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

Note A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes the purpose of the CLI interactive Help commands.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the Help feature in any command mode.
?	Lists all commands available for a particular command mode.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'. If nothing
matches, the help list will be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

***partial command*?**

```
Router(config)# zo?
zone  zone-pair
```

***partial command*<Tab>**

```
Router(config)# we<Tab> webvpn
```

***command* ?**

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

***command keyword* ?**

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name
Router(config)# ethernet cfm domain dname ?
  level
Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
  <cr>

Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>

Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a numeral. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a numeral for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see the following:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

Using the Command History Feature

The command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

  Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples are from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see the following:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.html

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or to disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode of the command-line interface.

The **no** form is documented in the command pages of Cisco IOS command references. The **default** form is generally documented in the command pages only when the **default** form performs a function different than that of the plain and **no** forms of the command.

Command pages often include a "Command Default" section as well. The "Command Default" section documents the state of the configuration if the command is not used (for configuration commands) or the outcome of using the command if none of the optional keywords or arguments is specified (for EXEC commands).

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference*:

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html

Caution Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

The following three output modifiers are available:

- **begin** *regular-expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular-expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular-expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression "protocol."

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at "^" marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the *Cisco IOS Release 12.4T System Message Guide*.

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved.

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
- Cisco Product/Technology Support

  http://www.cisco.com/go/techdocs
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)

  http://www.cisco.com/kobayashi/sw-center/
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

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.

© 2008–2010 Cisco Systems, Inc. All rights reserved.

Cisco IOS Switching Paths Overview

First Published: February 11, 2008
Last Updated: May 5, 2008

This module provides an overview of the switching paths that can be configured on Cisco IOS devices.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for the Cisco IOS Switching Paths Overview" section on page 10.

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

Information About IOS Switching Paths

This section provides information about Cisco IOS switching paths and contains the following concepts:

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

Basic Router Platform Architecture and Processes

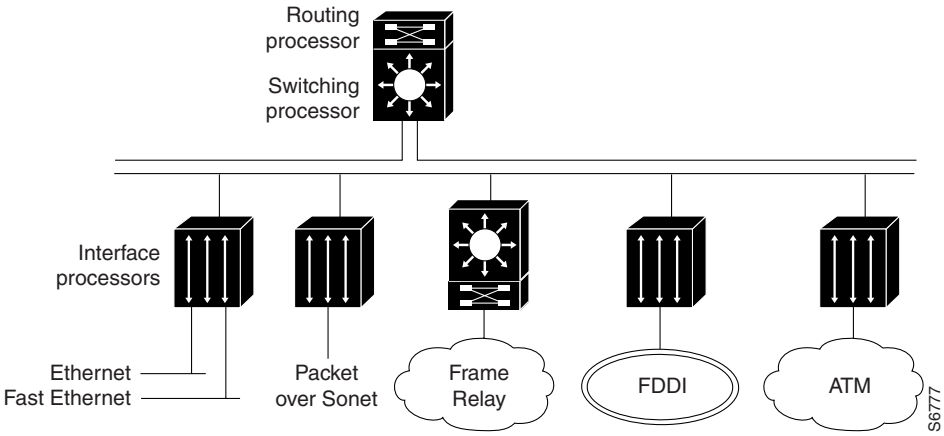
To understand how switching works, it helps to first understand the basic router architecture and where various processes occur in the router.

Note IP unicast fast switching is not supported on Cisco IOS 12.2S, 12.2SB, 12.2SR, and 12.2SX releases.

Fast switching is enabled by default on all interfaces that support fast switching. If you have a situation where you need to disable fast switching and fall back to the process-switching path, understanding how various processes affect the router and where they occur will help you determine your alternatives. This understanding is especially helpful when you are troubleshooting traffic problems or need to process packets that require special handling. Some diagnostic or control resources are not compatible with fast switching or come at the expense of processing and switching efficiency. Understanding the effects of those resources can help you minimize their effect on network performance.

Figure 1 illustrates a possible internal configuration of a Cisco 7500 series router. In this configuration, the Cisco 7500 series router has an integrated Route Switch Processor (RSP) and uses *route caching* to forward packets. The Cisco 7500 series router also uses Versatile Interface Processors (VIPs), a RISC-based interface processor that receives and caches routing information from the RSP. The VIP card uses the route cache to make switching decisions locally, which relieves the RSP of involvement and speeds overall throughput. This type of switching is called distributed switching. Multiple VIP cards can be installed in one router.

Figure 1 Basic Router Architecture



Cisco Routing and Switching Processes

The routing, or forwarding, function comprises two interrelated processes to move information in the network:

- Making a routing decision by routing
- Moving packets to the next hop destination by switching

Cisco IOS platforms perform both routing and switching, and there are several types of each:

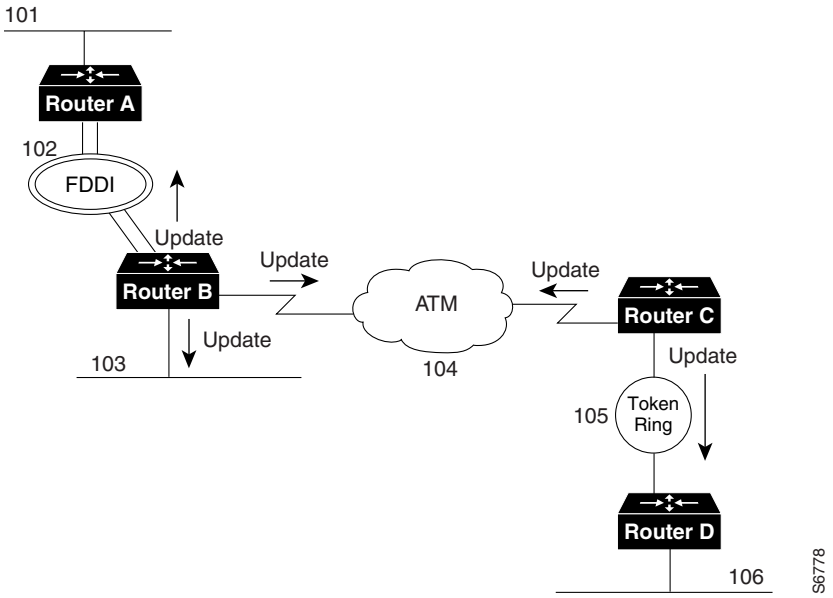
Routing Processes

The routing process assesses the source and destination of traffic based on knowledge of network conditions. Routing functions identify the best path to use for moving the traffic to the destination out one or more of the router interfaces. The routing decision is based on various criteria such as link speed, topological distance, and protocol. Each protocol maintains its own routing information.

Routing is more processing intensive and has higher latency than switching as it determines path and next hop considerations. The first packet routed requires a lookup in the routing table to determine the route. The route cache is populated after the first packet is routed by the route-table lookup. Subsequent traffic for the same destination is switched using the routing information stored in the route cache.

Figure 2 illustrates the basic routing process.

Figure 2 The Routing Process



A router sends routing updates out each of its interfaces that are configured for a particular protocol. It also receives routing updates from other attached routers. From these received updates and its knowledge of attached networks, it builds a map of the network topology.

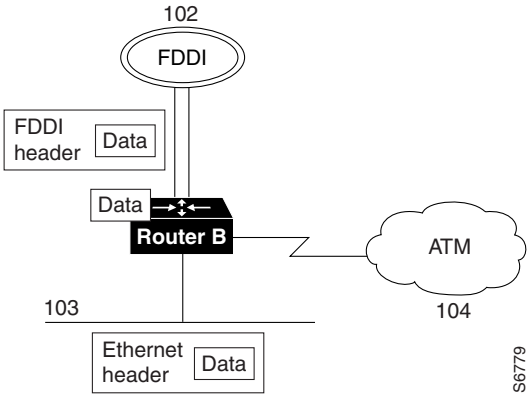
Selective Packet Discard Manages Routing Protocol Packets During Overload Conditions

When in severe overload conditions, routers that cannot keep up with the incoming packet stream must drop packets. If no intelligence is applied to choosing which packets to discard, the stability of routing protocols is impacted. The Selective Packet Discard (SPD) feature applies some simple choices to selectively discard packets likely to be unimportant for routing and interface stability. SPD is enabled by default; there are no commands or configuration tasks required.

Switching Processes

Through the switching process, the router determines the next hop toward the destination address. Switching moves traffic from an input interface to one or more output interfaces. Switching is optimized and has lower latency than routing because it can move packets, frames, or cells from buffer to buffer with simpler determination of the source and destination of the traffic. It saves resources because it does not involve extra lookups. Figure 3 illustrates the basic switching process.

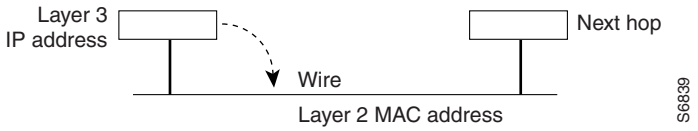
Figure 3 The Switching Process



In Figure 3, packets are received on the Fast Ethernet interface and destined for the FDDI interface. Based on information in the packet header and destination information stored in the routing table, the router determines the destination interface. It looks in the routing table of the protocol to discover the destination interface that services the destination address of the packet.

The destination address is stored in tables such as ARP tables for IP or AARP tables for AppleTalk. If there is no entry for the destination, the router will either drop the packet (and inform the user if the protocol provides that feature) or discover the destination address by some other address resolution process, such as through ARP. Layer 3 IP addressing information is mapped to the Layer 2 MAC address for the next hop. Figure 4 illustrates the mapping that occurs to determine the next hop.

Figure 4 *Layer 3-to-Layer 2 Mapping*



Basic Switching Paths

Basic switching paths are described in the following sections:

- Process Switching, page 5
- Fast Switching, page 5
- Cisco Express Forwarding Switching, page 5
- Distributed Cisco Express Forwarding Switching, page 6
- Platform and Switching Path Correlation, page 7

Process Switching

In process switching the first packet is copied to the system buffer. The router looks up the Layer 3 network address in the routing table and initializes the fast-switch cache. The frame is rewritten with the destination address and sent to the outgoing interface that services that destination. Subsequent packets for that destination are sent by the same switching path. The route processor computes the cyclical redundancy check (CRC).

Fast Switching

When packets are fast switched, the first packet is copied to packet memory and the destination network or host is found in the fast-switching cache. The frame is rewritten and sent to the outgoing interface that services the destination. Subsequent packets for the same destination use the same switching path. The interface processor computes the CRC. Fast switching is described in the *Configuring Fast Switching* module.

Note IP unicast fast switching is not supported is not supported on Cisco IOS 12.2S releases.

Cisco Express Forwarding Switching

When Cisco Express Forwarding mode is enabled, the Cisco Express Forwarding Forwarding Information Base (FIB) and adjacency tables reside on the Route Processor (RP), and the RP performs the express forwarding. You can use Cisco Express Forwarding mode 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. For information on configuring Cisco Express Forwarding, see the *Cisco Express Forwarding Overview* module.

Note Beginning with Cisco IOS Release 12.0, Cisco Express Forwarding is the preferred and default switching path. NetFlow switching has been integrated into Cisco Express Forwarding switching. For more information, see the *Cisco Express Forwarding Overview* module.

Distributed Cisco Express Forwarding Switching

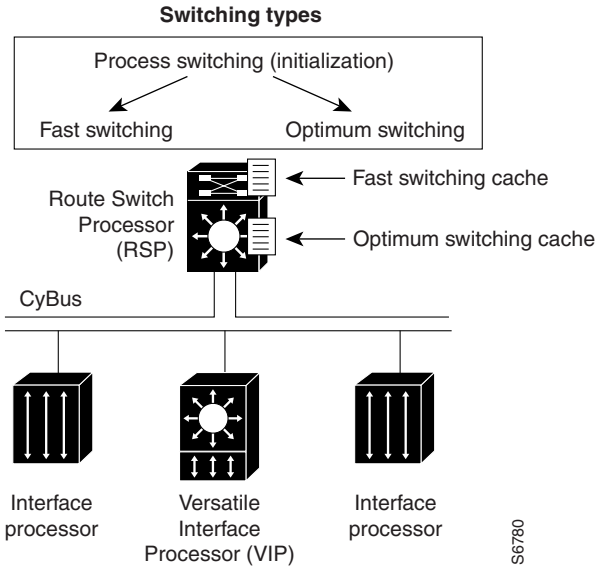
In distributed switching, the switching process occurs on VIP and other interface cards that support switching. When distributed Cisco Express Forwarding is enabled, line cards, such as VIP line cards or GSR line cards, maintain an identical copy of the FIB and adjacency tables. The line cards perform the express forwarding between port adapters, relieving the RSP of involvement in the switching operation. distributed Cisco Express Forwarding uses an Inter Process Communication (IPC) mechanism to ensure synchronization of FIBs and adjacency tables on the RP and line cards.

For model numbers and hardware compatibility information, refer to the *Cisco Product Catalog*. For information on configuring distributed Cisco Express Forwarding, see the *Cisco Express Forwarding Overview* module.

For information on configuring Multicast Distributed Switching (MDS), see the *Configuring Multicast Distributed Switching* module.

Figure 5 illustrates the distributed switching process on the Cisco 7500 series.

Figure 5 Distributed Switching on Cisco 7500 Series Routers



The VIP card installed in this router maintains a copy of the routing cache information needed to forward packets. Because the VIP card has the routing information it needs, it performs the switching locally, making the packet forwarding much faster. Router throughput is increased linearly based on the number of VIP cards installed in the router.

Platform and Switching Path Correlation

Depending on the routing platform you are using, availability and default implementations of switching paths varies. Table 1 shows the correlation between Cisco IOS switching paths and routing platforms.

Table 1 Switching Paths on Cisco 7200 and Cisco 7500 Series Routers

Switching Path	Cisco 7200 Series	Cisco 7500 Series	Comments	Configuration Command
Process switching	Yes	Yes	Initializes switching caches	**no** *protocol* **route-cache**
Fast switching	Yes	Yes	Default (except for IP unicast)	*protocol* **route-cache**
Cisco Express Forwarding switching	Yes	Yes	Default for IP	*protocol* **route-cache cef**
distributed Cisco Express Forwarding switching	No	Yes	Using second-generation VIP line cards	*protocol* **route-cache cef distributed**

Features That Affect Performance

Performance is derived from the switching mechanism you are using. Some Cisco IOS features require special handling and cannot be switched until the additional processing they require has been performed. This special handling is not processing that the interface processors can do. Because these features require additional processing, they affect switching performance. These features include the following:

- Queueing When Network Congestion Occurs, page 7
- Random Early Detection for Congestion Avoidance, page 8
- Compression Options Depending on Protocol You Are Using, page 8
- Filtering Using Access Lists, page 8
- Encryption Added For Security, page 8
- Accounting Feature Based on Protocol Used, page 8

For information on Quality of Service (QoS) performance, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Queueing When Network Congestion Occurs

Queueing occurs when network congestion occurs. When traffic is moving well within the network, packets are sent as they arrive at the interface. Cisco IOS software implements four different queueing algorithms as follows:

- FIFO queueing—Packets are forwarded in the same order in which they arrive at the interface.
- Priority queueing (PQ)—Packets are forwarded based on an assigned priority. You can create priority lists and groups to define rules for assigning packets to priority queues.

- Custom queueing (CQ)—You can control a percentage of interface bandwidth for specified traffic by creating protocol queue lists and custom queue lists.
- Weighted fair queueing (WFQ)—WFQ provides automatic traffic priority management. Low-bandwidth sessions have priority over high-bandwidth sessions. High-bandwidth sessions are assigned weights. WFQ is the default for interfaces slower than 2.048 Mbps.

Random Early Detection for Congestion Avoidance

Random Early Detection (RED) is designed for congestion avoidance. Traffic is prioritized based on type of service (ToS), or precedence. This feature is available on T3, OC-3, and ATM interfaces.

Compression Options Depending on Protocol You Are Using

Depending on the protocol you are using, various compression options are available in Cisco IOS software. Refer to the Cisco IOS configuration guide for the protocol you are using to learn compression options available.

Filtering Using Access Lists

You can define access lists to control access to or from a router for a number of services. You could, for example, define an access list to prevent packets with a certain IP address from leaving a particular interface on a router. How access lists are used depends on the protocol. For information on access lists, refer to the appropriate Cisco IOS configuration guide for the protocol you are using.

Encryption Added For Security

Encryption algorithms are applied to data to alter its appearance, making it incomprehensible to those not authorized to see the data. For information about encryption features available with the Cisco IOS software, refer to the *Cisco IOS Security Configuration Guide*.

Accounting Feature Based on Protocol Used

You can configure accounting features to collect network data related to resource usage. The information you collect (in the form of statistics) can be used for billing, chargeback, and planning resource usage. Refer to the appropriate Cisco IOS configuration guide for the protocol you are using for information regarding accounting features you can use.

How to Configure Cisco IOS Switching Paths Overview

Cisco IOS switching path overview has no configuration tasks.

Configuration Examples for Cisco IOS Switching Paths Overview

Cisco IOS switching path overview has no configuration tasks and therefore no configuration examples.

Additional References

The following sections provide references related to Cisco IOS Switching Paths.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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 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*
Tasks for configuring fast switching	*Configuring Fast Switching*
Tasks for configuring Multicast Distributed Switching	*Configuring Multicast Distributed Switching*

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
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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the Cisco IOS Switching Paths Overview

Table 2 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the "Cisco IOS IP Switching Features Roadmap" module.

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

Table 2 Feature Information for Cisco IOS Switching Paths Overview

Feature Name	Releases	Feature Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS Release 12.2(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 (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 (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. 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 Switch Processor (RSP) 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. For example, a Versatile Interface Processor (VIP) is a line card for the Cisco 7500 series router.

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).

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.

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. 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

Cisco Express Forwarding

Cisco Express Forwarding Features Roadmap

First Published: May 2, 2005
Last Updated: February 11, 2008

This feature roadmap lists the Cisco IOS features documented in the Cisco Express Forwarding modules in the *Cisco IOS IP Switching Configuration Guide* and maps them to the documents in which they appear. The roadmap is organized so that you can select your release train and see the features in that release. Find the feature name you are searching for and click on the URL in the "Where Documented" column to access the document containing that feature.

Feature and Release Support

Table 1 lists Cisco Express Forwarding feature support for the following Cisco IOS software release trains:

- Cisco IOS Release 12.2S
- Cisco IOS Release 12.2SB
- Cisco IOS Release 12.2SR
- Cisco IOS Release 12.2SX
- Cisco IOS Releases 12.2T, 12.3, 12.3T, 12.4, and 12.4T

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

Table 1 lists the most recent release of each software train first and the features in alphabetical order within the release.

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

© 2005—2008 Cisco Systems, Inc. All rights reserved.

Table 1 Supported Cisco Express Forwarding Features

Release	Feature Name	Feature Description	Where Documented
Cisco IOS Release 12.2S			
12.2(25)S	Cisco Express Forwarding: Command Changes	This feature details changes to command that are required to support Cisco Express Forwarding. In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, Cisco Express Forwarding has been updated to support new features and new hardware. These updates enable Cisco Express Forwarding to operate with the Multiprotocol Label Switching (MPLS) High Availability (HA) applications and the MPLS Forwarding Infrastructure (MFI).	"Cisco Express Forwarding: Command Changes"
Cisco IOS Release 12.2SB			
12.2(31)SB2	Cisco Express Forwarding—SNMP CEF-MIB Support	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.	"Cisco Express Forwarding—SNMP CEF-MIB Support"
12.2(28)SB	Cisco Express Forwarding: Command Changes	This feature details changes to command that are required to support Cisco Express Forwarding. In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, Cisco Express Forwarding has been updated to support new features and new hardware. These updates enable Cisco Express Forwarding to operate with the Multiprotocol Label Switching (MPLS) High Availability (HA) applications and the MPLS Forwarding Infrastructure (MFI).	"Cisco Express Forwarding: Command Changes"

Table 1 Supported Cisco Express Forwarding Features (continued)

Release	Feature Name	Feature Description	Where Documented
Cisco IOS Release 12.2SR			
12.2(33)SRC	Cisco Express Forwarding—SNMP CEF-MIB Support	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.	"Cisco Express Forwarding—SNMP CEF-MIB Support"
12/2(33)SRA	Cisco Express Forwarding: Command Changes	This feature details changes to command that are required to support Cisco Express Forwarding. In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, Cisco Express Forwarding has been updated to support new features and new hardware. These updates enable Cisco Express Forwarding to operate with the Multiprotocol Label Switching (MPLS) High Availability (HA) applications and the MPLS Forwarding Infrastructure (MFI).	"Cisco Express Forwarding: Command Changes"
Cisco IOS Release 12.2SX			
12.2(33)SXH	Cisco Express Forwarding: Command Changes	This feature details changes to command that are required to support Cisco Express Forwarding. In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, Cisco Express Forwarding has been updated to support new features and new hardware. These updates enable Cisco Express Forwarding to operate with the Multiprotocol Label Switching (MPLS) High Availability (HA) applications and the MPLS Forwarding Infrastructure (MFI).	"Cisco Express Forwarding: Command Changes"
Cisco IOS Releases 12.2T, 12.3, 12.3T, 12.4, and 12.4T			

Table 1 Supported Cisco Express Forwarding Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.4(20)T	Cisco Express Forwarding Enhancements: Removal of IP Fast Switching and Introduction of CLI Changes	The purpose of this document is to describe the changes based on the Cisco Express Forwarding infrastructure scalability enhancements implemented to adapt to the evolution of the Internet and to support new platforms and features. The changes are the removal of IP fast switching and the introduction of commands line interface (CLI) modifications. This document lists Cisco Express Forwarding CLI commands that are removed, replaced, new, and changed. The document lists and illustrates new commands, changed commands, and related command that are unchanged, to help you transition to the new CLI format. Enhancements to Cisco Express Forwarding enable it to operate with the Multiprotocol Label Switching (MPLS) Forwarding Infrastructure (MFI) and guarantees consistency between Cisco IOS release trains. Cisco Express Forwarding infrastructure changes were introduced and implemented in the Cisco IOS 12.2(25)S-based releases and added for T releases in Cisco IOS Release 12.4(20)T.	"Cisco Express Forwarding Enhancements: Removal of IP Fast Switching and Introduction of CLI Changes"
	Cisco Express Forwarding: Command Changes	This feature details changes to command that are required to support Cisco Express Forwarding. In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, Cisco Express Forwarding has been updated to support new features and new hardware. These updates enable Cisco Express Forwarding to operate with the Multiprotocol Label Switching (MPLS) High Availability (HA) applications and the MPLS Forwarding Infrastructure (MFI).	"Cisco Express Forwarding: Command Changes"
	Cisco Express Forwarding—SNMP CEF-MIB Support	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.	"Cisco Express Forwarding—SNMP CEF-MIB Support"

Table 1 Supported Cisco Express Forwarding Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.2(8)T	CEF-Switched Multipoint GRE Tunnels	This feature enables Cisco Express Forwarding 1switching of IP traffic to and from multipoint generic routing encapsulation (GRE) tunnels. Prior to the introduction of this feature, only process switching was available for multipoint GRE tunnels.	"Cisco Express Forwarding Overview"
12.2(8)T	Nonstop Forwarding Enhanced FIB Refresh	This feature allows you to clear the forwarding table on demand and to continue forwarding using the old entries in the table while the new forwarding table is being built.	"Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables"

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0807R)

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.

© 2005—2008 Cisco Systems, Inc. All rights reserved.

Cisco Express Forwarding Overview

First Published: May 2, 2005
Last Updated: June 11, 2008

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 feature information and caveats, see 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 for Cisco Express Forwarding Overview" section on page 13.

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

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

Information About Cisco Express Forwarding

Before using Cisco Express Forwarding or distributed Cisco Express Forwarding, you should understand the following:

Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding

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.

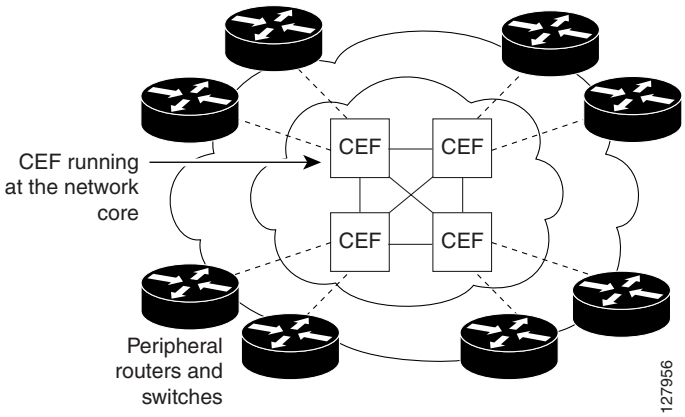
Cisco Express Forwarding Benefits: Improved Performance, Scalability, and Resilience

Cisco Express Forwarding offers the following 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, Figure 1 shows Cisco Express Forwarding being run on Cisco 12000 Series Internet 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



In a typical high-capacity Internet service provider (ISP) environment, Cisco 12000 Series Internet routers function as aggregation devices at the core of the network and support links to Cisco 7500 series routers or other feeder devices. Cisco Express Forwarding in these 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 Cisco Express Forwarding

Cisco Express Forwarding currently 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)
- TokenRing
- Tunnels

Main Components of Cisco Express Forwarding 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 when changes occur in the network and contains all routes known at the time. For more information, see the "FIB Overview" section on page 4.

Adjacency tables maintain Layer 2 next-hop addresses for all FIB entries. For more information, see the "Cisco Express Forwarding Adjacency Tables Overview" section on page 5.

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 invalidation of cache entries.

FIB Overview

Cisco Express Forwarding uses a 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.

Cisco Express Forwarding 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.

Cisco Express Forwarding 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, page 5
- Adjacency Types That Require Special Handling, page 5
- Unresolved Adjacency, page 6

Adjacency Discovery

Each adjacency table is populated as adjacencies are discovered. Adjacencies are added to the table either through indirect manual configuration or dynamically—discovered through a mechanism like Address Resolution Protocol (ARP) or 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 Table 1.

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 router is connected to a multiaccess medium, the FIB table on the router 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 router 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 router forwards packets that require special handling or packets sent by features that are not yet supported in conjunction with Cisco Express Forwarding switching paths to the next higher switching level for handling.
Discard adjacency	The router discards the packets.
Drop adjacency	The router 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.

Cisco Express Forwarding Operation Modes: Central and Distributed

Cisco Express Forwarding can be enabled in one of the two modes described in the following sections:

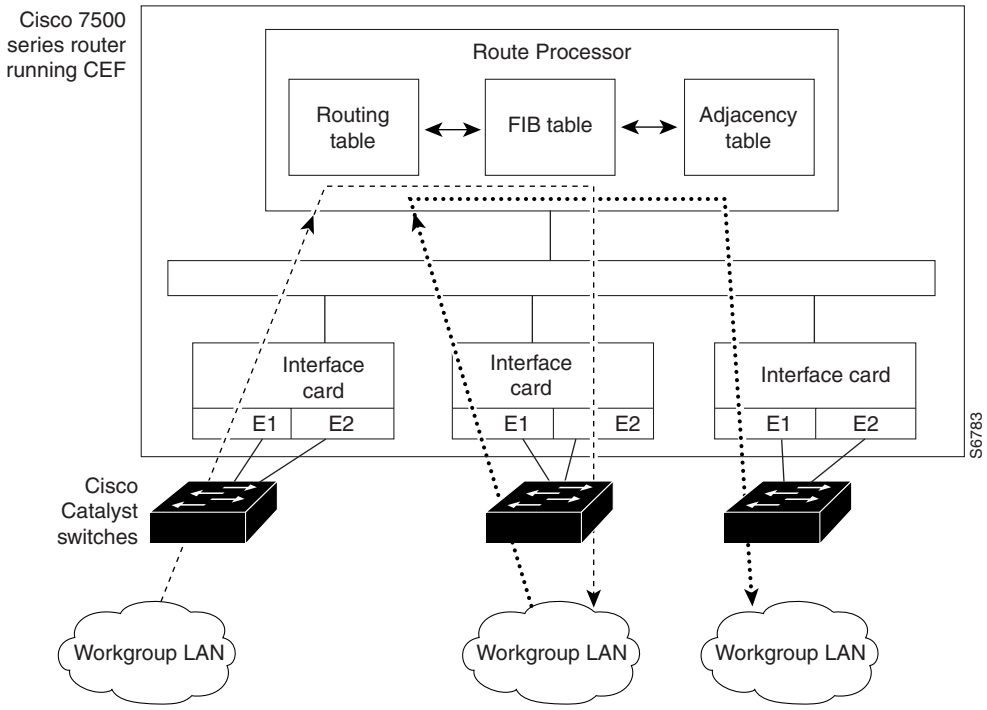
- Central Cisco Express Forwarding Mode Operation, page 6
- Distributed Cisco Express Forwarding Mode Operation, page 7

Central Cisco Express Forwarding 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.

Figure 2 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.

Figure 2 Central Cisco Express Forwarding Mode Operation



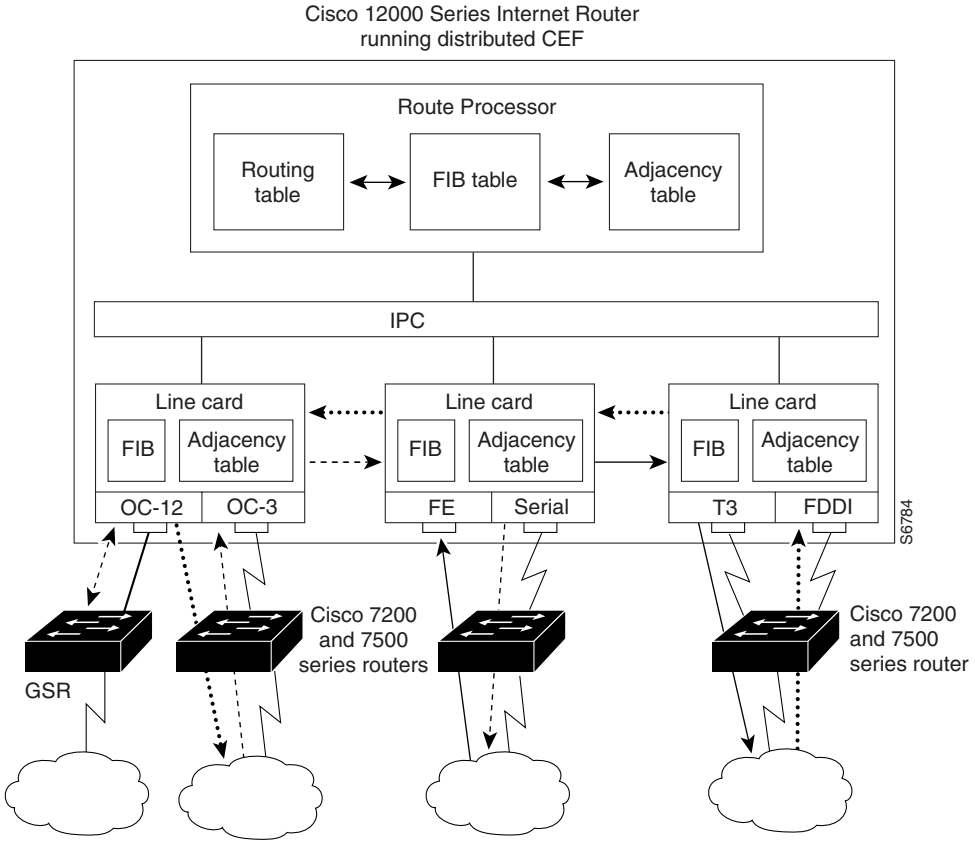
Distributed Cisco Express Forwarding Mode Operation

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.

Figure 3 shows the relationship between the RP and line cards when distributed Cisco Express Forwarding mode is active.

Figure 3 ***Distributed Cisco Express Forwarding Mode Operation***



In the Cisco 12000 Series Internet Router, shown in Figure 3, 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.

Cisco Express Forwarding Features Enabled by Default

The following features are enabled by default when Cisco Express Forwarding is enabled:

- Per-destination load balancing and the universal load sharing algorithm (see the "Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic" module)
- Distributed tunnel switching (see the "Cisco Express Forwarding Distributed Tunnel Switching" section on page 9)
- Multipoint generic routing encapsulation (GRE) tunnels (see the "Cisco Express Forwarding-Switched Multipoint GRE Tunnels (Cisco IOS 12.2(8)T)" section on page 9)

Cisco Express Forwarding Distributed Tunnel Switching

Cisco Express Forwarding supports distributed tunnel switching, such as that made possible by 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.

Cisco Express Forwarding-Switched Multipoint GRE Tunnels (Cisco IOS 12.2(8)T)

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 Cisco Express Forwarding Features

Table 2 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 Cisco Express Forwarding

There are no tasks for the Cisco Express Forwarding Overview module.

See the "Related Documents" section on page 10 for links to configuration information for Cisco Express Forwarding features and services.

Configuration Examples for Cisco Express Forwarding

There are no configuration examples for the Cisco Express Forwarding Overview module.

See the "Related Documents" section on page 10 for links to configuration information for Cisco Express Forwarding features and services.

Where to Go Next

See the "Related Documents" section on page 10 for links to configuration information for Cisco Express Forwarding features and services.

Additional References

The following sections provide references related to configuring Cisco Express Forwarding.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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*

Related Topic	Document Title
Tasks for customizing the display of recorded Cisco Express Forwarding events	*Customizing the Display of Recorded Cisco Express Forwarding Events*
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

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco Express Forwarding Overview

Table 3 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

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. • "Cisco Express Forwarding-Switched Multipoint GRE Tunnels (Cisco IOS 12.2(8)T)" section on page 9
CEF Support for IP Routing between IEEE 802.1Q vLANs	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005 – 2008 Cisco Systems, Inc. All rights reserved.

Configuring Basic Cisco Express Forwarding for Improved Performance, Scalability, and Resiliency in Dynamic Networks

First Published: May 2, 2005
Last Updated: July 11, 2008

This module contains information about Cisco Express Forwarding and describes the required and optional tasks for verifying Cisco Express Forwarding and distributed 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 feature information and caveats, see 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 for Configuring Basic Cisco Express Forwarding" section on page 29.

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.

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

Contents

Prerequisites for Configuring Cisco Express Forwarding

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

Restrictions for Configuring Cisco Express Forwarding

Cisco Express Forwarding has the following restrictions:

- The Cisco 12000 Series Internet routers operate only in distributed Cisco Express Forwardingmode.
- 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 Configuring Basic Cisco Express Forwarding

Before using Cisco Express Forwarding or distributed Cisco Express Forwarding, you should understand the following:

- Cisco Platform Support for Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 3
- Cisco Express Forwarding Benefits: Improved Performance, Scalability, and Resiliency, page 3
- Main Components for Cisco Express Forwarding Operation, page 4
- Cisco Express Forward Operation Modes: Central and Distributed, page 4
- How to Configure Basic Cisco Express Forwarding, page 7

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 on page 26 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 CEF operation on interfaces that are using IEEE 802.1Q encapsulation on VLAN subinterfaces.

Cisco Platform Support for Cisco Express Forwarding and Distributed Cisco Express Forwarding

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

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       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 Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

Cisco Express Forwarding Benefits: Improved Performance, Scalability, and Resiliency

Cisco Express Forwarding offers the following 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 Cisco Express Forwarding 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.

Cisco Express Forward Operation Modes: Central and Distributed

Cisco Express Forwarding can be enabled in one of the two modes described in the following sections:

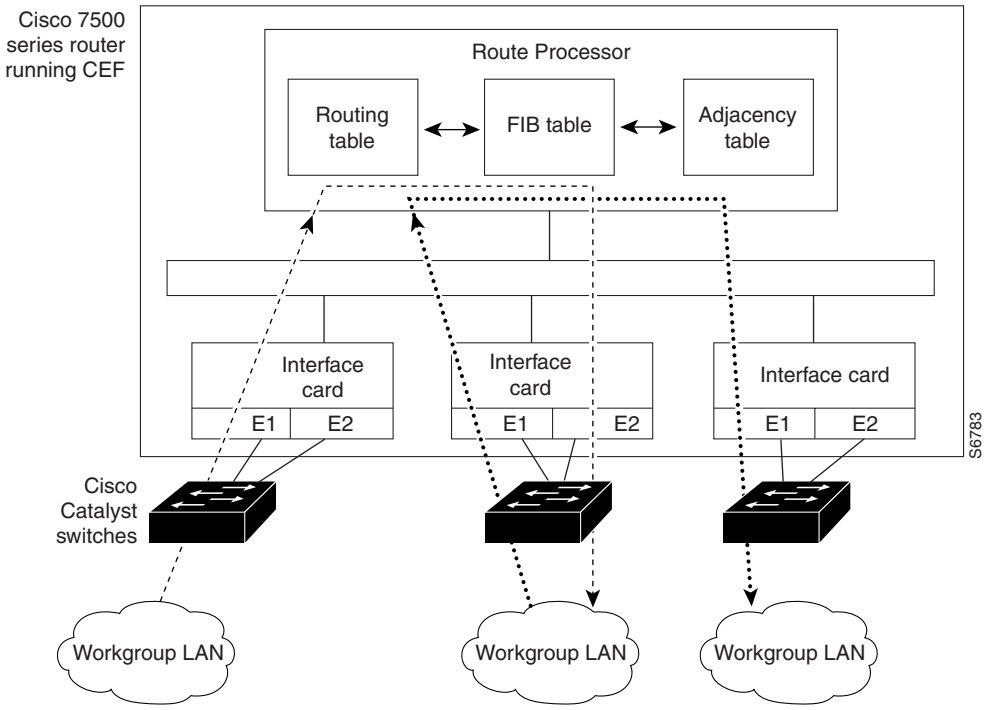
- Central Cisco Express Forwarding Mode Operation, page 4
- Distributed Cisco Express Forwarding Mode Operation, page 5

Central Cisco Express Forwarding 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 platform that is not a distributed 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.

Figure 1 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.

Figure 1 Central Cisco Express Forwarding Mode Operation



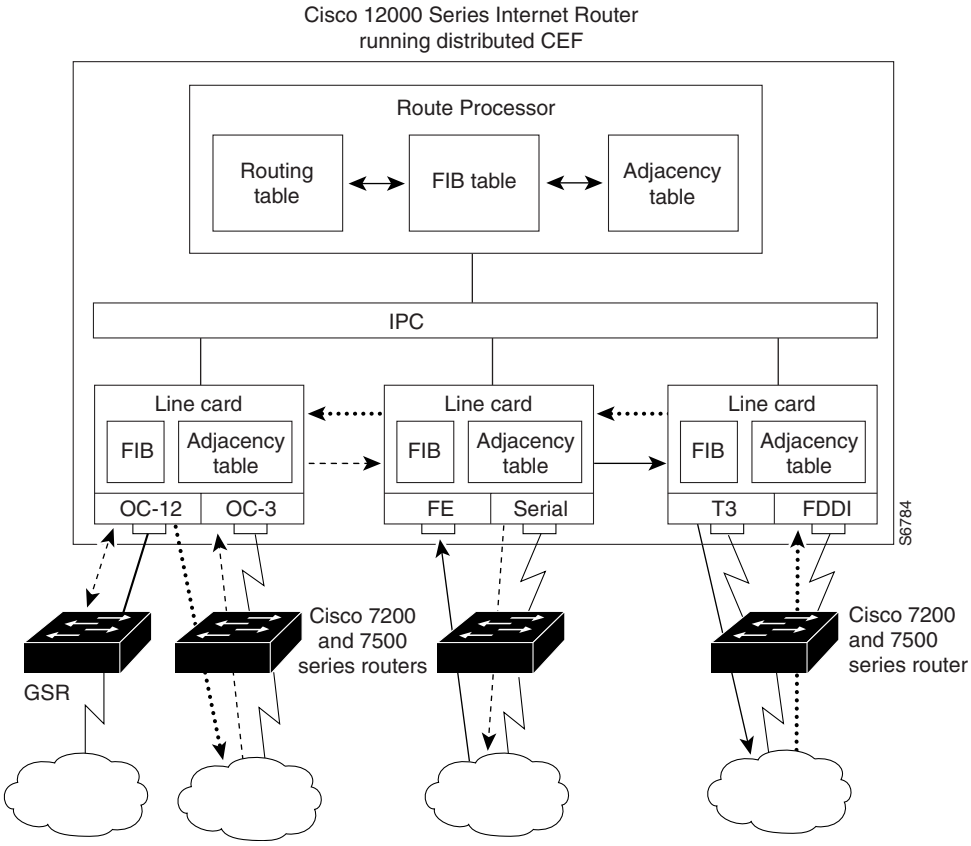
Distributed Cisco Express Forwarding Mode Operation

For additional scalability, Cisco Express Forwarding runs in the form of distributed Cisco Express Forwarding 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.

Figure 2 shows the relationship between the RP and line cards when distributed Cisco Express Forwarding mode is active.

Figure 2 Distributed Cisco Express Forwarding Mode Operation



In the Cisco 12000 Series Internet Router, shown in Figure 2, 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.

How to Configure Basic Cisco Express Forwarding

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

How to Verify Basic Cisco Express Forwarding

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. Cisco Express Forwarding is enabled by default on the Cisco 7100, 7200, and 7500 series routers. Distributed Cisco Express Forwarding is enabled by default on the Catalyst 6500 switch and on Cisco 12000 Series Internet 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 If the Router Is Configured for Central or Distributed Cisco Express Forwarding, page 7 (required)
- Verifying Cisco Express Forwarding Operation on Your Router, page 8 (optional)
- Verifying Distributed Cisco Express Forwarding Operation on Your Router, page 15 (optional)
- Interpreting Information in Cisco Express Forwarding Command Output, page 21 (optional)

Determining If the Router Is Configured for Central or Distributed Cisco Express Forwarding

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 number*] [**brief**]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`show ip interface`** [*type number*] [**`brief`**] **Example:** `Router# show ip interface`	Displays the usability status of interfaces configured for IP. • The *type* argument is the interface type. • The *number* argument is the interface number. • The **brief** keyword displays a summary of the usability status information. Look for the entry "IP CEF switching enabled" or "IP Distributed CEF switching enabled."
Step 3	**`exit`** **Example:** `Router# exit`	Exits to user EXEC mode.

What to Do Next

- If the router is configured for Cisco Express Forwarding, complete the steps in each of the tasks on the RP in the "Verifying Cisco Express Forwarding Operation on Your Router" section on page 8.
- If the router is configured for distributed Cisco Express Forwarding, complete the steps in each of the tasks on the line card in the "Verifying Distributed Cisco Express Forwarding Operation on Your Router" section on page 15. You might also need to complete steps, as indicated in each task, on the RP. By performing the same steps on the RP that you do on the line cards, you can verify that the forwarding tables on the RP and the line cards are synchronized.

Verifying Cisco Express Forwarding Operation on Your Router

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:

- Verifying That Cisco Express Forwarding Switching Is Enabled on the Input Interface on the Router, page 9
- Locating the Prefix in a Forwarding Table on the RP, page 10
- Finding the Cisco Express Forwarding Output Information Associated with the Prefix on the RP, page 12
- Verifying the Adjacency or Next-Hop Information on the RP, page 13

See the "Verifying Distributed Cisco Express Forwarding Operation on Your Router" section on page 15 for the tasks to perform for d istributed Cisco Express Forwarding operation.

Verifying That Cisco Express Forwarding Switching Is Enabled on the Input Interface on the Router

To verify tha 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 number* **detail**
4. **show ip interface** *type number*
5. **exit**

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:

```
Router> enable
Router#
```

Step 2 **show ip cef**

Use this command to verify that Cisco Express Forwarding is enabled globally. For 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 number* **detail**

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:

```
Router# show cef interface fastethernet 1/0/0 detail

FastEthernet1/0/0 is up (if_number 9)
  Corresponding hwidb fast_if_number 9
  Corresponding hwidb firstsw->if_number 9
  Internet address is 10.2.61.8/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is FastEthernet1/0/0
  Fast switching type 1, interface type 5
  IP CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
```

```
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A82 (0x48001A82)
  IP MTU 1500
```

Step 4 **show ip interface** *type number*

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

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 **exit**

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

```
Router# exit
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. **exit**

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:

```
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:

```
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
[...]
```

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:

```
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            Ethernet1/3
10.2.0.0/8          10.0.0.2            POS6/0
10.0.0.0/8          attached            Ethernet1/3
10.0.0.0/32         receive
10.0.0.1/32         10.0.0.1            Ethernet1/3
10.0.0.2/32         receive
10.255.255.255/32   receive
10.3.0.0/8          10.0.0.2            POS6/0
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 **exit**

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

```
Router# exit
Router>
```

Finding the Cisco Express Forwarding Output Information Associated with the Prefix on the RP

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. **exit**

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:

```
Router> enable
Router#
```

Step 2 **show ip cef**

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

```
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, FastEthernet6/1 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:

```
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, FastEthernet6/1 via 192.168.101.1/32
    valid adjacency
  0 packets, 0 bytes switched through the prefix
```

Step 5 **exit**

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

```
Router# exit
Router>
```

Verifying the Adjacency or Next-Hop Information on the RP

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 number*
6. **show ip cef exact-route** *source-address destination-address*
7. **exit**

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:

```
Router> enable
Router#
```

Step 2 **show ip cef**

Use this command to find the output interface. For 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:

```
Router# show adjacency detail

Protocol Interface                 Address
IP       Ethernet1/0/0             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 an Ethernet 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:

```
Router# show adjacency summary

Adjacency Table has 1 adjacency
  Interface                 Adjacency Count
  Ethernet1/0/0             1
```

Step 5 **show adjacency** *type number*

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

```
Router# show adjacency fastethernet 2/3

Protocol  Interface                  Address
IP        FastEthernet2/3            172.20.52.1(3045)
IP        FastEthernet2/3            172.20.52.22(11)
```

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:

```
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 Ethernet1/0/0 to next hop address 192.168.100.1.

Step 7 **exit**

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

```
Router# exit
Router>
```

Verifying Distributed Cisco Express Forwarding Operation on Your Router

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

- Verifying That Distributed Cisco Express Forwarding Switching Is Enabled on the Input Interface on a Line Card, page 15
- Locating the Prefix in a Forwarding Table on a Line Card, page 16
- Finding the Distributed Cisco Express Forwarding Output Information Associated with the Prefix on a Line Card, page 18
- Verifying the Adjacency or Next-Hop Information on a Line Card, page 19

Syntax for Cisco Express Forwarding Commands on Line Cards

To perform tasks on router line cards, you need to use the following syntax: **execute-on** [**slot** *slot-number* | **all**] *command*. The **execute-on** commands apply only to the Cisco 12000 Series Internet routers and the Cisco 7500 series routers. The **all** keyword is available only on the Cisco 12000 Series Internet routers.

For example, use the following command to display FIB entries on the line cards in the first slot:

```
Router# execute-on 0 show ip cef
```

To perform tasks on a Catalyst 6500 series switch, you use the following syntax: **remote command module** *mod command*. For example:

```
Router# remote command module 2 show ip cef
```

The tasks in this document apply to the Cisco 7500 series and Cisco 12000 Series Internet routers.

Verifying That Distributed Cisco Express Forwarding Switching Is Enabled on the Input Interface on a Line Card

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. **execute-on slot** *slot-number* **show ip cef** *prefix*
4. **exit**

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:

```
Router> enable
Router#
```

Step 2 **show ip cef**

Use this command to verify that Cisco Express Forwarding is enabled globally. For 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 **execute-on slot** *slot-number* **show ip cef** *prefix*

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

```
Router# execute-on slot 0 show ip cef 192.68.0.0 255.255.255.0

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 Ethernet5/0/0, 0 dependencies
    valid glean adjacency
```

Step 4 **exit**

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

```
Router# exit
Router>
```

Locating the Prefix in a Forwarding Table on a Line Card

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

SUMMARY STEPS

1. **enable**
2. **execute-on slot** *slot-number* **show ip cef**
3. **execute-on all show ip cef** ***vrf*** *vrf-name*
4. Repeat Step 2 as many times as required to locate the prefix.
5. **show ip cef**
6. **exit**

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:

```
Router> enable
Router#
```

Step 2 **execute-on slot** *slot-number* **show ip cef**

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

```
Router# execute-on slot 0 show ip cef

show ip cef from slot 0:

Prefix              Next Hop            Interface
0.0.0.0/0            192.168.0.1         Ethernet5/0/0
0.0.0.0/32           receive
192.168.0.0/24       attached            Ethernet5/0/0
192.168.0.0/32       receive
192.168.0.1/32       192.168.0.1         Ethernet5/0/0
192.168.0.141/32     receive
192.168.0.255/32     receive
239.224.0.0/4        drop
239.224.0.0/24       receive
255.255.255.255/32   receive
```

Step 3 **execute-on all show ip cef vrf** *vrf-name*

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

```
Router# execute-on all show ip cef vrf vpn1

Prefix              Next Hop            Interface
0.0.0.0/32          receive
10.1.0.0/8          10.0.0.1            Ethernet1/3
10.2.0.0/8          10.0.0.2            POS6/0
10.0.0.0/8          attached            Ethernet1/3
10.0.0.0/32         receive
10.0.0.1/32         10.0.0.1            Ethernet1/3
10.0.0.2/32         receive
10.255.255.255/32   receive
10.3.0.0/8          10.0.0.2            POS6/0
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 distributed Cisco Express Forwarding is in a VPN, you might need to look at multiple VRFs.

Step 5 **show ip cef**

Use this command to show entries in the FIB on the RP and to verify that the FIB on the line card is synchronized with the FIB maintained by the router. For 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       FastEthernet6/1
[...]
```

Compare the prefixes, next hops, and interfaces in this output with those in the output from Step 1 to verify that FIB on the line card is synchronized with the FIB maintained by the router.

Step 6 **exit**

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

```
Router# exit
Router>
```

Finding the Distributed Cisco Express Forwarding Output Information Associated with the Prefix on a Line Card

To find the distributed Cisco Express Forwarding output information associated with the prefix on a line card, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **execute-on slot** *slot-number* **show ip cef**
3. **execute-on slot** *slot-number* **show ip cef** *prefix*
4. **execute-on slot** *slot-number* **show ip cef** *prefix* **detail**
5. **exit**

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:

```
Router> enable
Router#
```

Step 2 **execute-on slot** *slot-number* **show ip cef**

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

```
Router# execute-on slot 0 show ip cef

show ip cef from slot 0:

Prefix              Next Hop            Interface
0.0.0.0/0           192.168.0.1          Ethernet5/0/0
0.0.0.0/32          receive
192.168.0.0/24      attached             Ethernet5/0/0
192.168.0.0/32      receive
192.168.0.1/32      192.168.0.1          Ethernet5/0/0
192.168.0.141/32    receive
192.168.0.255/32    receive
239.224.0.0/4       drop
239.224.0.0/24      receive
255.255.255.255/32  receive
```

Step 3 **execute-on slot** *slot-number* **show ip cef** *prefix*

Use this command to display the prefix entry in the FIB on a line card. For example:

```
Router# execute-on slot 3 show ip cef 192.68.0.0 255.255.255.0

show ip cef 192.168.0.0 255.255.255.0 from slot 0:

192.168.0.0/24, version 19, epoch 0, attached, connected
0 packets, 0 bytes
  via Ethernet5/0/0, 0 dependencies
    valid glean adjacency
```

Step 4 **execute-on slot** *slot-number* **show ip cef** *prefix* **detail**

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

```
Router# execute-on slot 0 show ip cef 10.24.48.32 detail

show ip cef 192.168.0.0 255.255.255.0 from slot 0:

192.168.0.0/24, version 19, epoch 0, attached, connected
0 packets, 0 bytes
  via Ethernet5/0/0, 0 dependencies
    valid glean adjacency
```

Step 5 **exit**

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

```
Router# exit
Router>
```

Verifying the Adjacency or Next-Hop Information on a Line Card

To verify the adjacency or next-hop information on a line card, perform the following steps.

Cisco Express Forwarding adds an adjacency to the adjacency table when the adjacency is

- Indirectly configured manually
- Dynamically discovered through ARP
- Created when a routing protocol, for example, BGP or 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 number*
6. **show ip cef exact-route** *source-address destination-address*

7. **execute-on all show ip cef** *destination*
8. **exit**

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:

```
Router> enable
Router#
```

Step 2 **show ip cef**

Use this command to determine the output interface. For 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:

```
Router# show adjacency detail

Protocol Interface                 Address
IP       Ethernet1/0/0             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 an Ethernet link by means of Ethernet II encapsulation. (The first 12 characters are the MAC address of the destination next-hop interface. The next 12 characters represent the MAC address of the source interface of the packet. The last 4 characters [0x0800] represent the Ethernet II encapsulation value for IP.)

Step 4 **show adjacency summary**

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

```
Router# show adjacency summary

Adjacency Table has 1 adjacency
  Interface                 Adjacency Count
  Ethernet1/0/0             1
```

Step 5 **show adjacency** *type number*

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

```
Router# show adjacency fastethernet 2/3
```

```
Protocol  Interface                 Address
IP        FastEthernet2/3           172.20.52.1(3045)
IP        FastEthernet2/3           172.20.52.22(11)
```

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:

```
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 Ethernet1/0/0 to next hop address 192.168.100.1.

Step 7 **execute-on all show ip cef** *destination*

Use this command to display output interfaces and next hops for all line cards. For example:

```
Router# execute-on all show ip cef 10.20.84.32

========= Line Card (Slot 1) =======
10.16.0.0/13, version 408935, cached adjacency 0.0.0.0
0 packets, 0 bytes
Flow: AS 6172, mask 13
via 172.16.213.1, 0 dependencies, recursive
next hop 172.16.213.1, POS1/0.500 via 172.16.213.0/30
valid cached adjacency

========= Line Card (Slot 2) =======
10.16.0.0/13, version 13719, cached adjacency 0.0.0.0
0 packets, 0 bytes
Flow: AS 6172, mask 13
via 172.16.213.1, 0 dependencies, recursive
next hop 172.16.213.1, POS1/0.500 via 172.16.213.0/30
valid cached adjacency
```

Step 8 **exit**

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

```
Router# exit
Router>
```

Interpreting Information in Cisco Express Forwarding Command Output

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

- Verifying That the Cisco Express Forwarding Information Looks As Expected, page 22 (optional)
- Interpreting MPLS Information in Cisco Express Forwarding Output, page 24 (optional)

Verifying That the Cisco Express Forwarding 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 1 and 2.
5. **execute-on slot** *slot-number* **show ip cef**
6. Compare the command output in Steps 2 and 4.
7. **exit**

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:

```
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:

```
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, Fddi0/0/0
O    192.168.92.0/24 [110/2] via 10.5.5.5, 00:00:04, POS2/0/0
```

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:

```
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           Fddi0/0/0
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           Fddi0/0/0
10.23.64.0/24       10.150.3.9           Fddi0/0/0
10.23.66.0/24       10.150.3.9           Fddi0/0/0(normal route)
10.47.0.10/32       10.150.3.9           Fddi0/0/0
10.150.3.0/24       attached             Fddi0/0/0
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           Fddi0/0/0
172.16.57.0/24      10.5.5.5             POS2/0/0
                    10.150.3.9           Fddi0/0/0
239.224.0.0/4       receive(multicast)
255.255.255.255/32  receive(all 1s broadcast)
```

Step 4 Compare the command output in Steps 1 and 2.

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 1 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 1:

  ```
  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 2:

  ```
  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) **execute-on slot** *slot-number* **show ip cef**

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

```
Router# execute-on slot 2 show ip cef

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           Fddi0/0/0
```

```
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          Fddi0/0/0
10.7.54.0/24        attached            Fddi0/1/0
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          Fddi0/0/0
10.23.66.0/24       10.150.3.9          Fddi0/0/0
10.47.0.10/32       10.150.3.9          Fddi0/0/0
10.150.3.0/24       attached            Fddi0/0/0
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          Fddi0/0/0
172.16.57.0/24      10.5.5.5            POS2/0/0
                    10.150.3.9          Fddi0/0/0
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 2 should be identical to the output from the **execute-on slot 2 show ip cef** command in Step 4. 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 **exit**

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

```
Router# exit
Router>
```

Interpreting MPLS Information in Cisco Express Forwarding Output

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

Cisco Express Forwarding and MPLS Interaction

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 Versatile Interface Processor (VIP) or to line cards in the same way that the FIB tables are distributed in Cisco Express Forwarding.

MPLS VPNs and Cisco Express Forwarding Tables

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. **exit**

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:

```
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:

```
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.

```
  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."

```
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 **exit**

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

```
Router# exit
Router>
```

Configuration Examples for Basic Cisco Express Forwarding

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.*

Additional References

The following sections provide references related to configuring basic Cisco Express Forwarding.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*

Related Topic	Document Title
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/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*
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*
QoS features that require Cisco Express Forwarding	*When Is CEF Required for Quality of Service*

Standards

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Basic Cisco Express Forwarding

Table 1 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

Table 1 Feature Information for Configuring Basic Cisco Express Forwarding

Feature Name	Releases	Feature Configuration Information
CEF/dCEF - Cisco Express Forwarding	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

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 (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. 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 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. 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.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005—2008 Cisco Systems, Inc. All rights reserved.

Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding to Customize Switching and Forwarding for Dynamic Networks

First Published: May 2, 2005
Last Updated: July 11, 2008

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 feature information and caveats, see 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 for Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding" section on page 13.

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.

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

Contents

Prerequisites for Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding

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 Cisco Express Forwarding or Distributed Cisco Express Forwarding

Central Cisco Express Forwarding or distributed Cisco Express Forwarding has the following restrictions:

- The Cisco 12000 Series Internet routers operate 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.
- Distributed Cisco Express Forwarding switching cannot be configured on the same Versatile Interface Processor (VIP) card on which distributed fast switching is configured.
- Distributed Cisco Express Forwarding is not supported on Cisco 7200 series routers.

Restrictions for Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation on an Interface

- On the Cisco 12000 Series Internet Router, you must not disable distributed Cisco Express Forwarding on an interface.
- Not all switching methods are available on all platforms.

Information About Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding

Before enabling or disabling Cisco Express Forwarding or distributed Cisco Express Forwarding, you should understand the following:

- Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 3
- When to Enable or Disable Central Cisco Express Forwarding Operation on a Router, page 4
- When to Enable Distributed Cisco Express Forwarding Operation on a Line Card, page 4
- When to Enable or Disable Cisco Express Forwarding Operation on an Interface, page 4

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features you can configure, refer to the following section:

- How to Enable or Disable Central Cisco Express Forwarding or Distributed Cisco Express Forwarding, page 5

Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding

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.

When to Enable or Disable Central Cisco Express Forwarding Operation 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 Distributed Cisco Express Forwarding Operation 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, such as the VIP line cards or the Cisco 12000 Series Internet Router 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 12000 Series Internet 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 Cisco Express Forwarding Operation 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 software switches packets received on the interface using the next fastest switching path. For Cisco Express Forwarding, the next fastest switching path is fast 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 switching path that a packet takes. Consider the following rules of thumb 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.
- In contrast, because Cisco IOS builds a fast-switching cache entry after switching a packet, a packet coming in on a process-switched interface and going out through a fast-switched interface is fast switched.
- If you want to disable fast switching, use the **no ip route-cache** command on the egress interface.

How to Enable or Disable Central Cisco Express Forwarding or Distributed Cisco Express Forwarding

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 Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation on a Router, page 5 (optional)
- Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation on an Interface, page 7 (optional)

Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation 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*] [**unresolved** [**detail**]] | [**detail** | **summary**]]
3. **configure terminal**

4. **[no] ip cef**
   or
   [no] ip cef distributed
5. **exit**
6. **show ip cef** [**vrf** *vrf-name*] [**unresolved** [**detail**] | [**detail** | **summary**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip cef** [**vrf** *vrf-name*] [**unresolved** [**detail**]] | [**detail** | [**summary**]] **Example:** `Router# show ip cef`	Displays entries in the forwarding information base (FIB). 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: `%CEF not running`
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 4	[**NO**] **ip cef**
	or
	[**NO**] **ip cef distributed**
	
	Example:
	`Router(config)# ip cef`
	or
	
	Example:
	`Router(config)# ip cef distributed`
		Enables Cisco Express Forwarding on the route processor card.
		or
		Enables distributed Cisco Express Forwarding operation. Cisco Express Forwarding information is distributed to line cards. Line cards perform express forwarding.

Step 5	**exit** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.
Step 6	**show ip cef** [**vrf** *vrf-name*] [**unresolved** [**detail**] | [**detail** | **summary**]] **Example:** `Router# show ip cef`	Displays entries in the FIB. 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 Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation 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 number*] [**statistics**] [**detail**]
3. **configure terminal**
4. **interface** *type slot/port* or **interface** *type slot/port-adapter/port*
5. [**no**] **ip route-cache cef** or **ip route-cache cef**

   or

   [**no**] **ip route-cache distributed**
6. **end**
7. **show cef interface** [*type number*] [**statistics**] [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cef interface** [*type number*] [**statistics**] [**detail**] **Example:** `Router# show cef interface fastethernet 1/0/0`	Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces. Look for “IP CEF switching enabled” or “IP Distributed CEF switching enabled” in the output.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 4	**interface** type slot/port or **interface** type slot/port-adapter/port **Example:** Router(config)# interface ethernet 1/1 or Router(config)# interface fastethernet 1/0/0	Configures an interface type and enters interface configuration mode. • The *type* argument specifies the type of interface to be configured. • The *slot/* argument specifies the slot number. Refer to the appropriate hardware manual for slot and port information. • The *port* argument specifies the port number. Refer to the appropriate hardware manual for slot and port information. • The *port-adapter/* argument specifies the port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.
Step 5	[**no**] **ip route-cache cef** or [**no**] **ip route-cache distributed** **Example:** Router(config-if)# no ip route-cache cef or **Example:** Router(config-if)# no ip route-cache distributed	Disables Cisco Express Forwarding operation on an interface or enables Cisco Express Forwarding operation on an interface after Cisco Express Forwarding operation was disabled. or Disables distributed Cisco Express Forwarding operation on an interface or enables distributed Cisco Express Forwarding operation on an interface after distributed Cisco Express Forwarding operation was disabled.
Step 6	**end** **Example:** Router(config)# end	Exits to privileged EXEC mode.
Step 7	**show cef interface** [*type number*] [**statistics**] [**detail**] **Example:** Router# show cef interface fastethernet 1/0/0	Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces. Verify that "IP CEF switching enabled" or "IP Distributed CEF switching enabled" is displayed in the output.

Configuration Examples for Enabling or Disabling Central Cisco Express Forwarding or Distributed Cisco Express Forwarding

This section contains the following configuration examples:

- Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation: Examples, page 9
- Enabling or Disabling Central Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation on an Interface: Examples, page 9

Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation: Examples

Cisco Express Forwarding is enabled by default on the Cisco 7100, 7200, and 7500 series routers. You might want to disable Cisco Express Forwarding if your router and router interfaces are configured with a feature that Cisco Express Forwarding does not support. The following example shows how to disable Cisco Express Forwarding on a router and on all interfaces on the router:

```
configure terminal
!
no ip cef
end
```

Distributed Cisco Express Forwarding is enabled by default on the Cisco 6500 and 12000 series routers. The following example shows how to enable distributed Cisco Express Forwarding on the line cards of a router, such as the Cisco 7500 series router, that supports distributed Cisco Express Forwarding:

```
configure terminal
!
ip cef distributed
end
```

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
```

Enabling or Disabling Central Cisco Express Forwarding or Distributed Cisco Express Forwarding Operation on an Interface: Examples

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
 no ip route-cache cef
 end
```

The following example shows how to reenable central Cisco Express Forwarding operation on an interface:

```
configure terminal
!
interface ethernet 1/1
 ip route-cache cef
 end
```

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

```
configure terminal
!
interface e0
 no ip route-cache distributed
 end
```

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

```
configure terminal
!
ip cef distributed
!
interface e0
# ip route-cache distributed
 end
```

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

```
configure terminal
!

ip cef
!
interface e0
 no 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 Ethernet interface 0:

```
configure terminal
!
ip cef distributed

interface e0
 no ip route-cache cef
 end
```

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

```
configure terminal
!
ip cef distributed
!
interface e0
 ip route-cache distributed
 end
```

Additional References

The following sections provide references related to enabling or disabling central Cisco Express Forwarding or distributed Cisco Express Forwarding.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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*
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*
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*
QoS features that require Cisco Express Forwarding	*When Is CEF Required for Quality of Service*
Cisco Express Forwarding command changes for MPLS HA application and the MFI infrastructure in Cisco IOS 12.2S releases	*Cisco Express Forwarding: Command Changes*

Standards

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Enabling or Disabling Cisco Express Forwarding or Distributed Cisco Express Forwarding

Table 1 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

Table 1 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 Release 12.2(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 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005–2008 Cisco Systems, Inc. All rights reserved.

Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic

First Published: May 2, 2005
Last Updated: July 11, 2008

This module contains information about Cisco Express Forwarding and describes the required and optional 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 feature information and caveats, see 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 for Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic" section on page 16.

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

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

Prerequisites for Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic

- 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 Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic

You must globally configure load balancing on Cisco 12000 Series Router E2 line cards in the same way: either in per-destination or per-packet mode. It is not possible (as in other Cisco IOS software-based platforms) to configure some packet prefixes in per-destination mode and others in per-packet mode.

Information About Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic

Before configuring a load-balancing scheme for Cisco Express Forwarding traffic, you should understand the following concepts:

- Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 3
- Cisco Express Forwarding Load-Balancing Overview, page 3
- Per-Destination Load Balancing for Cisco Express Forwarding Traffic, page 3
- Per-Packet Load Balancing for Cisco Express Forwarding Traffic, page 4
- Load-Balancing Algorithms for Cisco Express Forwarding Traffic, page 4

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features that you can configure, see the "Additional References" section on page 13.

Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding

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 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 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 for Cisco Express Forwarding Traffic

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.

Note The Cisco 10000 series router and the Cisco 12000 series router are configured by default to perform per-destination load balancing.

Per-Packet Load Balancing for Cisco Express Forwarding Traffic

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.

Load-Balancing Algorithms for Cisco Express Forwarding Traffic

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. The include-ports algorithm is available in Cisco IOS Release 12.4(11)T and later releases.

How to Configure a Load-Balancing Scheme for Cisco Express Forwarding Traffic

Perform the following tasks to configure and fine-tune load balancing for Cisco Express Forwarding:

- Enabling or Disabling Cisco Express Forwarding Per-Destination Load Balancing, page 5 (optional)
- Configuring Cisco Express Forwarding Per-Packet Load Balancing, page 6 (optional)
- Selecting a Cisco Express Forwarding Load-Balancing Algorithm, page 7 (optional)

Enabling or Disabling Cisco Express Forwarding 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. **interface** *type slot/port* or **interface** *type slot/port-adapter/port*
4. [**no**] **ip cef load-sharing** [**per-packet**] [**per-destination**]
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	**interface** type slot/port or **interface** type slot/port-adapter/port **Example:** Router(config)# interface ethernet 1/1 or **Example:** Router(config)# interface fastethernet 1/0/0	Configures an interface type and enters interface configuration mode. • The *type* argument specifies the type of interface to be configured. • The *slot* argument specifies the slot number. Refer to the appropriate hardware manual for slot and port information. • The *port* argument specifies the port number. Refer to the appropriate hardware manual for slot and port information. • The *port-adapter* argument specifies the port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility. **Note** The slashes after the *slot* argument and *port-adapter* argument are required.
Step 4	[**no**] **ip cef load-sharing** [**per-packet**] [**per-destination**] **Example:** Router(config-if)# no ip cef load-sharing per-destination	Enables load balancing for Cisco Express Forwarding. • The **no ip cef load-sharing** command disables Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic load balancing. • The **per-packet** keyword enables per-packet load balancing on the interface. • The **per-destination** keyword enables per-destination load balancing on the interface.
Step 5	**end** **Example:** Router(config-if)# end	Exits to privileged EXEC mode.

Configuring Cisco Express Forwarding 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. **interface** *type slot/port* or **interface** *type slot/port-adapter/port*
4. [**no**] **ip load-sharing** [**per-packet**] [**per-destination**]
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.

Step 3	**interface** type slot/port
	or
	interface type slot/port-adapter/port
	
	Example:
	`Router(config)# interface ethernet 1/1`
	or
	`Router(config)# interface fastethernet 1/0/0`
		Configures an interface type and enters interface configuration mode.
		• The *type* argument specifies the type of interface to be configured.
		• The *slot* argument specifies the slot number. Refer to the appropriate hardware manual for slot and port information.
		• The *port* argument specifies the port number. Refer to the appropriate hardware manual for slot and port information.
		• The *port-adapter* argument specifies the port adapter number. Refer to the appropriate hardware manual for information about port adapters.
		Note The slashes after the *slot* argument and *port-adapter* argument are required.

Step 4	[**no**] **ip load-sharing** [**per-packet**] [**per-destination**] **Example:** `Router(config-if)# ip load-sharing per-packet`	Enables load balancing for Cisco Express Forwarding. • The **per-packet** keyword enables per-packet load balancing on the interface. • The **per-destination** keyword enables per-destination load balancing on the interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Selecting a Cisco Express Forwarding Load-Balancing Algorithm

Perform one of the following tasks to elect a Cisco Express Forwarding load-balancing algorithm.

- Selecting a Tunnel Load-Balancing Algorithm for Cisco Express Forwarding Traffic, page 8
- Selecting an Include-Ports Layer 4 Load-Balancing Algorithm for Cisco Express Forwarding Traffic, page 9

The router is set to perform universal load sharing by default.

Selecting a Tunnel Load-Balancing Algorithm for Cisco Express Forwarding Traffic

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`** **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	**ip cef load-sharing algorithm** {**original** | **tunnel** [*id*] | **universal** [*id*] | **include-ports** {**source** [*id*] | [**destination**] [*id*] | **source** [*id*] **destination** [*id*]}} **Example:** `Router(config)# ip cef load-sharing algorithm tunnel`	Selects a Cisco Express Forwarding load-balancing algorithm. • The **original** keyword sets the load-balancing algorithm to the original algorithm, based on a source and destination hash. • 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. • The *id* argument is a fixed identifier. • The **universal** keyword sets the load-balancing algorithm to one that uses a source and destination and an ID hash. • The **include-ports source** keywords set the load-balancing algorithm to one that uses the source port. • The **include-ports destination** keywords set the load-balancing algorithm to one that uses the destination port. • The **include-ports source destination** keywords set the load-balancing algorithm to one that uses both source and destination ports.
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Selecting an Include-Ports Layer 4 Load-Balancing Algorithm for Cisco Express Forwarding Traffic

Perform the following task to select an include-ports load-balancing algorithm for Cisco Express Forwarding traffic. Select the include-port algorithm when your network environment contains traffic running over equal-cost paths that is not load shared because the majority of the traffic is between peer addresses with different port numbers, such as RTP streams.

Prerequisites

Your system must be using an image that supports Cisco Express Forwarding in Cisco IOS Release 12.4(11)T or a later release.

Restrictions

The Layer 4 load-balancing algorithm applies to software switched packets.

For platforms that switch traffic using a hardware forwarding engine, the hardware load-balancing decision might be different from the software load-balancing decision for the same traffic stream. You might want to override the configured algorithm.

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`** **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	**ip cef load-sharing algorithm** {**original** | **tunnel** [*id*] | **universal** [*id*] **include-ports** {**source** [*id*] | [**destination**] [*id*] | **source** [*id*] **destination** [*id*]}} **Example:** `Router(config)# ip cef load-sharing algorithm include-ports source destination`	Selects a Cisco Express Forwarding load-balancing algorithm. • The **original** keyword sets the load-balancing algorithm to the original algorithm, based on a source and destination hash. • 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. • The *id* argument is a fixed identifier. • The **universal** keyword sets the load-balancing algorithm to one that uses a source and destination and an ID hash. • The **include-ports source** keyword sets the load-balancing algorithm to one that uses the source port. • The **include-ports destination** keyword sets the load-balancing algorithm to one that uses the destination port. • The **include-ports source destination** keyword sets the load-balancing algorithm to one that uses the source and destination ports.
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged mode.

Configuration Examples for Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic

This section provides the following examples for configuring a load-balancing scheme for Cisco Express Forwarding traffic:

- Enabling or Disabling Cisco Express Forwarding Per-Destination Load Balancing: Example, page 12
- Configuring Cisco Express Forwarding Per-Packet Load Balancing: Example, page 12
- Selecting a Cisco Express Forwarding Load-Balancing Algorithm: Example, page 12

Enabling or Disabling Cisco Express Forwarding Per-Destination Load Balancing: Example

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
```

Configuring Cisco Express Forwarding Per-Packet Load Balancing: Example

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.

Selecting a Cisco Express Forwarding Load-Balancing Algorithm: Example

The router is set to perform universal load balancing by default.

The following examples show how to select a different Cisco Express Forwarding load-balancing algorithm:

- Selecting a Tunnel Load-Balancing Algorithm for Cisco Express Forwarding Traffic: Example, page 12
- Selecting an Include-Ports Layer 4 Load-Balancing Algorithm for Cisco Express Forwarding Traffic: Example, page 13

Selecting a Tunnel Load-Balancing Algorithm for Cisco Express Forwarding Traffic: Example

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
```

Selecting an Include-Ports Layer 4 Load-Balancing Algorithm for Cisco Express Forwarding Traffic: Example

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

The following sections provide references related to configuring a load-balancing scheme for Cisco Express Forwarding traffic.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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 Networks*
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
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

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic

Table 1 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

Table 1 Feature Information for Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic

Feature Name	Releases	Feature Configuration Information
Cisco Express Forwarding Support for Layer 4 Port-Based Load Balancing	12.4(11)T	This feature allows Cisco Express Forwarding to include Layer 4 port information in the decision for load sharing on equal cost paths. In 12.4(11)T, this feature was introduced. The following sections provide information about this feature: • Load-Balancing Algorithms for Cisco Express Forwarding Traffic, page 4 • Selecting a Cisco Express Forwarding Load-Balancing Algorithm, page 7 The following commands were modified by this feature: **ip cef load-sharing algorithm** and **show ip cef exact-route**.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005—2008 Cisco Systems, Inc. All rights reserved.

Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables

First Published: May 2, 2005
Last Updated: February 11, 2008

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 feature information and caveats, see 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 for Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables" section on page 13.

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

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

Prerequisites for Configuring Basic Cisco Express Forwarding

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

Information About Configuring Basic Cisco Express Forwarding

Tasks for configuring epochs for Cisco Express Forwarding Forwarding Information Base (FIB) tables were introduced with the Nonstop Forwarding Enhanced FIB Refresh feature in Cisco IOS Release 12.2(8)T.

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

- Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 2
- Nonstop Forwarding Enhanced FIB Refresh (Cisco IOS 12.2(8)T), page 3
- Epoch Numbering for Cisco Express Forwarding FIB and Adjacency Tables, page 3
- Epoch Synchronization Between the RP and Line Cards, page 4
- Epoch Numbering for Routers That Support High Availability, page 4
- When to Refresh the Cisco Express Forwarding or Adjacency Tables, page 4

(See the "Nonstop Forwarding Enhanced FIB Refresh (Cisco IOS 12.2(8)T)" section on page 3 for an explanation of the term "epoch.")

Tasks for configuring epochs for Cisco Express Forwarding tables were introduced with the Nonstop Forwarding Enhanced FIB Refresh feature in Cisco IOS Release 12.2(8)T.

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features you can configure, refer to the "Additional References" section on page 10.

Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding

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.

Nonstop Forwarding Enhanced FIB Refresh (Cisco IOS 12.2(8)T)

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 Cisco Express Forwarding 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 Cisco Express Forwarding or Adjacency Tables" section on page 4 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 High Availability

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 Cisco Express Forwarding or Adjacency Tables

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

Cisco 7500 series and Cisco 12000 Series Internet 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 and Verify Epoch Information for Cisco Express Forwarding Tables

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:

- Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table, page 5 (optional)
- Beginning a New Epoch and Incrementing the Epoch Number of One or All Cisco Express Forwarding Tables, page 6 (optional)
- Verifying Epoch Information for Cisco Express Forwarding and Adjacency Tables, page 7 (optional)

Beginning a New Epoch and 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 ip cef epoch**
3. **clear adjacency table**
4. **show ip cef epoch**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`show ip cef epoch`** **Example:** `Router# show ip cef epoch`	Displays entries in the forwarding information base (FIB) or displays a summary of the FIB. • The **epoch** keyword displays the table epochs of the adjacency table and all FIB tables.
Step 3	**`clear adjacency table`** **Example:** `Router# clear adjacency table`	Begins a new epoch and increments the epoch number of the adjacency table.

	Command or Action	Purpose
Step 4	**show ip cef epoch** **Example:** `Router# show ip cef epoch`	Displays entries in the FIB or displays a summary of the FIB. • The **epoch** keyword displays the table epochs of the adjacency table and all FIB tables.
Step 5	**exit** **Example:** `Router# exit`	Exits to user EXEC mode.

Beginning a New Epoch and Incrementing the Epoch Number of One or All Cisco Express Forwarding 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 ip cef epoch** command when you want to rebuild a Cisco Express Forwarding table. This command increments the epoch and flushes entries associated with the old epoch. This command also clears any inconsistencies that might exist between Cisco Express Forwarding tables on the PR and Cisco Express Forwarding tables on the line cards. If everything in the system is working correctly, the command has no effect on the Cisco Express Forwarding forwarding tables, other than changing the current epoch values.

SUMMARY STEPS

1. **enable**
2. **show ip cef epoch**]
3. **clear ip cef epoch** [**all-vrfs** | **full** | **vrf** [*table*]]
4. **show ip cef epoch**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip cef epoch** **Example:** `Router# show ip cef epoch`	Displays entries in the FIB or displays a summary of the FIB. • The **epoch** keyword displays the table epochs of the adjacency table and all FIB tables.

	Command or Action	Purpose
Step 3	**clear ip cef epoch** [**all-vrfs** | **full** | **vrf** [*table*]] **Example:** `Router# clear ip cef epoch full`	Begins a new epoch and increments the epoch number of one or all Cisco Express Forwarding tables. • The **all-vrfs** keyword begins a new epoch for all FIB tables. • The **full** keyword begins a new epoch for all tables, including adjacency tables. • The **vrf** keyword begins a new epoch for the specified FIB table. • The *table* argument is the name of a specific Virtual Private Network (VPN) routing and forwarding instance (VRF).
Step 4	**show ip cef epoch** **Example:** `Router# show ip cef epoch`	Displays entries in the FIB or displays a summary of the FIB. • The **epoch** keyword displays the epochs of the adjacency table and all FIB tables.
Step 5	**exit** **Example:** `Router# exit`	Exits to user EXEC mode.

Verifying Epoch Information for Cisco Express Forwarding and Adjacency Tables

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. For 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:

```
Router# show adjacency detail

Protocol Interface                 Address
IP       Serial5/0/0/1:1           point2point(7)
                                   0 packets, 0 bytes
                                   0F000800
                                   CEF   expires: 00:02:09
                                         refresh: 00:00:09
                                   Epoch: 14
IP       Serial5/0/1/1:1           point2point(7)
                                   0 packets, 0 bytes
                                   0F000800
                                   CEF   expires: 00:02:09
                                         refresh: 00:00:09
                                   Epoch: 14
```

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:

```
Router# show adjacency summary

Adjacency Table has 2 adjacencies
  Table epoch: 14 (2 entries at this epoch)

  Interface                 Adjacency Count
Serial5/0/0/1:1           1
Serial5/0/1/1:1           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, including the adjacency table, is as you expect.

In the following example, Cisco Express Forwarding epoch information is verified for all FIB tables, including the adjacency table:

```
Router# show ip cef epoch

CEF epoch information:

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

Adjacency table
  Table epoch: 16 (2 entries at this epoch)
```

Step 5 **exit**

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

```
Router# exit
Router>
```

Configuration Examples for Configuring Basic Cisco Express Forwarding

This section contains the following epoch configuration examples:

- Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table: Example, page 9
- Beginning a New Epoch and Incrementing the Epoch Number of One or All Cisco Express Forwarding Tables: Examples, page 9

Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table: Example

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)
```

Beginning a New Epoch and Incrementing the Epoch Number of One or All Cisco Express Forwarding Tables: Examples

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

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

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

CEF epoch information:

Table: Default-table
     Table epoch: 3 (43 entries at this epoch)

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

After clearing:

```
router# clear ip cef epoch full

router# show ip cef epoch

CEF epoch information:

Table: Default-table
     Table epoch: 4 (43 entries at this epoch)

Adjacency table
     Table epoch: 4 (5 entries at this epoch)
```

Additional References

The following sections provide references related to configuring epochs for Cisco Express Forwarding tables.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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 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 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*
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*
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*
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*

Standards

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Epochs to Clear and Rebuild Cisco Express Forwarding and Adjacency Tables

Table 1 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

Table 1 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	12.2(8)T	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. The following sections provide information about this feature: • Nonstop Forwarding Enhanced FIB Refresh (Cisco IOS 12.2(8)T), page 3 • Epoch Numbering for Cisco Express Forwarding FIB and Adjacency Tables, page 3 • Epoch Synchronization Between the RP and Line Cards, page 4 • Epoch Numbering for Routers That Support High Availability, page 4 • When to Refresh the Cisco Express Forwarding or Adjacency Tables, page 4 • Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table, page 5 • Beginning a New Epoch and Incrementing the Epoch Number of One or All Cisco Express Forwarding Tables, page 6 • Verifying Epoch Information for Cisco Express Forwarding and Adjacency Tables, page 7

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.

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.

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. Sometimes called CiscoBus controller.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005—2008 Cisco Systems, Inc. All rights reserved.

Configuring Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards

First Published: May 2, 2005
Last Updated: February 11, 2008

This module contains information about and instructions for configuring Cisco Express Forwarding consistency checkers for route processors and line cards. Cisco Express Forwarding consistency checkers help you 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 that occur and by issuing 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 feature information and caveats, see 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 for Configuring Basic Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards" section on page 11.

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.

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

Contents

Prerequisites for Configuring Basic Cisco Express Forwarding

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

Restrictions for Configuring Basic Cisco Express Forwarding

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

Information About Configuring Basic Cisco Express Forwarding

Before configuring Cisco Express Forwarding consistency checkers, you should understand the following:

- Cisco Platform Support for Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 2
- Cisco Express Forwarding Consistency Checker Types for Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 3

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features that you can configure, refer to the following section:

- How to Configure Cisco Express Forwarding Consistency Checkers, page 4

Cisco Platform Support for Cisco Express Forwarding and Distributed Cisco Express Forwarding

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 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 Cisco Express Forwarding or the **ip cef distributed** command to enable distributed Cisco Express Forwarding.

Cisco Express Forwarding Consistency Checker Types for Cisco Express Forwarding and Distributed Cisco Express Forwarding

Cisco Express Forwarding uses routing information that is retrieved from the Routing Information Base (RIB), the RP, and the line card databases to perform express forwarding. As these databases are updated, inconsistencies might result, due to the asynchronous nature of the distribution mechanism for these databases. 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. Table 1 describes the consistency checkers and indicates whether the checker operates on the RP or the line card.

Table 1 Types of Cisco Express Forwarding Consistency Checkers

Checker Type	Operates On	Description
Lc-detect	Line card	(Distributed Cisco Express Forwarding only) Retrieves IP prefixes found missing from the line card FIB table. If IP prefixes are missing, the line card cannot forward packets for the corresponding addresses. Lc-detect 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. Also, the RP sends a signal back to the line card confirming that the IP prefix contributes to the creation of an inconsistency.
Scan-lc	Line card	(Distributed Cisco Express Forwarding only) Looks through the FIB table for a configurable time period and sends the next *n* 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. The RP sends a signal back to the line card for confirmation. The time period and number of prefixes sent are configured with the **ip cef table consistency-check** command.
Scan-rp	Route Processor	Looks through the RP FIB table for a configurable time period and sends the next *n* prefixes to the line card. (This action is opposite to the one that the scan-lc 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. The time period and number of prefixes sent are configured with the **ip cef table consistency-check** command.
Scan-rib	Route Processor	Operates on all (even nondistributed) RPs, and scans the RIB to ensure that prefix entries are present in the RP FIB table.

Cisco Express Forwarding consistency checkers are enabled by default for Cisco IOS Releases 12.0(20)S and later. 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 it by examining the Cisco Express Forwarding system error messages and by issuing Cisco Express Forwarding **debug** and **show** commands.

For Cisco Express Forwarding consistency checker system error messages, see the *System Message Guide* for your Cisco IOS Release.

How to Configure Cisco Express Forwarding Consistency Checkers

Perform the following tasks to configure Cisco Express Forwarding consistency checkers:

- Enabling Cisco Express Forwarding Consistency Checkers, page 5 (optional)
- Displaying and Clearing Cisco Express Forwarding Table Inconsistencies, page 6 (optional)

Enabling Cisco Express Forwarding Consistency Checkers

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef table consistency-check** [**type** {**lc-detect** | **scan-lc** | **scan-rib** | **scan-rp**}] [**count** *count-number*] [**period** *seconds*]
4. **ip cef table consistency-check** [**settle-time** *seconds*]
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.
Step 3	**ip cef table consistency-check** [**type** {**lc-detect** | **scan-lc** | **scan-rib** | **scan-rp**}] [**count** *count-number*] [**period** *seconds*] **Example:** `Router(config)# ip cef table consistency-check scan-rib count 100 period 60`	Enables Cisco Express Forwarding table consistency checker types and parameters. • The **type** keyword indicates the type of consistency check to enable. • The **lc-detect** keyword enables the line card to detect a missing prefix, which is confirmed by the RP. • The **scan-lc** keyword enables a passive scan check of tables on the line card. • The **scan-rib** keyword enables a passive scan check of tables on the RP and a comparison with the RIB. • The **scan-rp** keyword enables a passive scan check of tables on the RP. • The **count**-*number* keyword-argument pair is the maximum number of prefixes to check per scan. The range is from 1 to 225. • The **period** *seconds* keyword-argument pair is the time during which updates for a candidate prefix are ignored as inconsistencies. The range is from 1 to 3600 seconds.

	Command or Action	Purpose
Step 4	**ip cef table consistency-check** [**settle-time** *seconds*] **Example:** `Router(config)# ip cef table consistency-check settle-time 65`	Suppresses inconsistency errors during route updates. • The **settle-time** *seconds* keyword-argument pair is the time elapsed during which updates for a candidate prefix are ignored as inconsistencies. The range is from 1 to 3600 seconds.
Step 5	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Displaying and Clearing Cisco Express Forwarding Table Inconsistencies

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

SUMMARY STEPS

1. **enable**
2. **show ip cef inconsistency**
3. **clear ip cef inconsistency**
4. **clear cef linecard** [*slot-number*] [**adjacency** | **interface** | **prefix**]
5. **show ip cef inconsistency**
6. **exit**

DETAILED STEPS

Step 1 **enable**

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

```
Router> enable
```

Enter your password if prompted.

Step 2 **show ip cef inconsistency**

Use this command to display Cisco Express Forwarding IP inconsistencies. For example:

```
Router# show ip cef inconsistency

Table consistency checkers (settle time 65s)
 lc-detect:running
 0/0/0 queries sent/ignored/received
 scan-lc:running [100 prefixes checked every 60s]
 0/0/0 queries sent/ignored/received
 scan-rp:running [100 prefixes checked every 60s]
 0/0/0 queries sent/ignored/received
 scan-rib:running [100 prefixes checked every 60s]
 0/0/0 queries sent/ignored/received
Inconsistencies:0 confirmed, 0/16 recorded
```

For each checker type, the output shows the number of prefixes that Cisco Express Forwarding must check and the number of seconds (the settle time) during which an inconsistency between RP and line card tables is ignored. The preceding output shows that 0 inconsistencies existed between these tables at the time the command was entered on the router.

Step 3 **clear ip cef inconsistency**

Use this command to clear the Cisco Express Forwarding inconsistency statistics and records found by the Cisco Express Forwarding consistency checkers. For example:

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

Step 4 **clear cef linecard** [*slot-number*] [**adjacency** | **interface** | **prefix**]

Use this command to clear Cisco Express Forwarding information from line cards. For example:

```
Router# clear cef linecard
```

Step 5 **show ip cef inconsistency**

Use this command to verify that Cisco Express Forwarding statistics on inconsistencies are removed from the RP and the line cards. For example:

```
Router# show ip cef inconsistency

Table consistency checkers (settle time 65s)
 lc-detect:running
  0/0/0 queries sent/ignored/received
 scan-lc:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
 scan-rp:running [100 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
 scan-rib:running [1000 prefixes checked every 60s]
  0/0/0 queries sent/ignored/received
Inconsistencies:0 confirmed, 0/16 recorded
```

This sample output shows that four consistency checkers are enabled, that each checker sends 100 prefixes to be checked every 60 seconds, and that the time during which inconsistencies are ignored is 65 seconds. In this example, no inconsistencies were found.

Step 6 **exit**

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

```
Router# exit
Router>
```

Configuration Examples for Configuring Basic Cisco Express Forwarding

This section contains the following Cisco Express Forwarding consistency checker configuration example:

- Enabling Cisco Express Forwarding Consistency Checkers: Example, page 8

Enabling Cisco Express Forwarding Consistency Checkers: Example

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

```
configure terminal
!
ip cef table consistency-check scan-rp count 225 period 3600
ip cef table consistency-check settle-time 2500
end
```

The RP is configured to send 3600 prefixes to the line cards every 225 seconds. After the prefixes are sent, the line cards is to wait 2500 seconds before signaling the PR to report an inconsistency (if there is one).

Additional References

The following sections provide references related to configuring Cisco Express Forwarding consistency checkers.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
Troubleshooting tips for incomplete adjacencies	*Troubleshooting Incomplete Adjacencies with CEF*
Description of and troubleshooting information for the consistency checker available for the Cisco 7500 series and Cisco 12000 Series Internet routers	*Troubleshooting Prefix Inconsistencies with Cisco Express Forwarding*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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 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 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*

Related Topic	Document Title
Tasks for customizing the display of recorded Cisco Express Forwarding events	*Customizing the Display of Recorded Cisco Express Forwarding Events*
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*

Standards

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Basic Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards

Table 2 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

Table 2 Feature Information for Configuring Basic Cisco Express Forwarding Consistency Checkers for Route Processors and Line Cards

Feature Name	Releases	Feature Configuration Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS Release 12.2(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 Forwarding—A mode of Cisco Express Forwarding switching 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.

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.

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.

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.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005—2008 Cisco Systems, Inc. All rights reserved.

Configuring Cisco Express Forwarding Network Accounting

First Published: May 2, 2005
Last Updated: February 11, 2008

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 feature information and caveats, see 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 for Configuring Cisco Express Forwarding Network Accounting" section on page 27.

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

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

Prerequisites for Configuring Cisco Express Forwarding 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 Cisco Express Forwarding and Distributed Cisco Express Forwarding" section for information on how to determine if Cisco Express Forwarding is enabled on your networking device.

Information About Configuring Cisco Express Forwarding Network Accounting

Before you configure Cisco Express Forwarding network accounting, you should understand the following information:

- Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 2
- Traffic Matrix Statistics That You Can Collect and View, page 3
- TMS and Cisco Express Forwarding Nonrecursive Accounting in Backbone Routers, page 4
- How Backbone Routers Collect TMS, page 5
- TMS Viewing Options, page 6

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features that you can configure, go to the "Additional References" section on page 24.

Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding

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.

Central Cisco Express Forwarding or distributed Cisco Express Forwarding has the following restrictions:

- The Cisco 12000 Series Internet routers operate only in distributed Cisco Express Forwarding mode. On these routers, you must not disable distributed Cisco Express Forwarding on an interface.
- 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.
- Distributed Cisco Express Forwarding switching cannot be configured on the same VIP card on which distributed fast switching is configured.
- Distributed Cisco Express Forwarding is not supported on Cisco 7200 series routers.

See the "Additional References" section on page 24 for links to more information on the features and functionality of Cisco Express Forwarding.

Traffic Matrix Statistics That You Can Collect and View

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 Cisco Express Forwarding Nonrecursive Accounting in Backbone Routers

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. Figure 1 and Figure 2 help illustrate the traffic statistics you can gather using TMS.

Figure 1 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.

Figure 1 Sample Network with Backbone Routers and Links

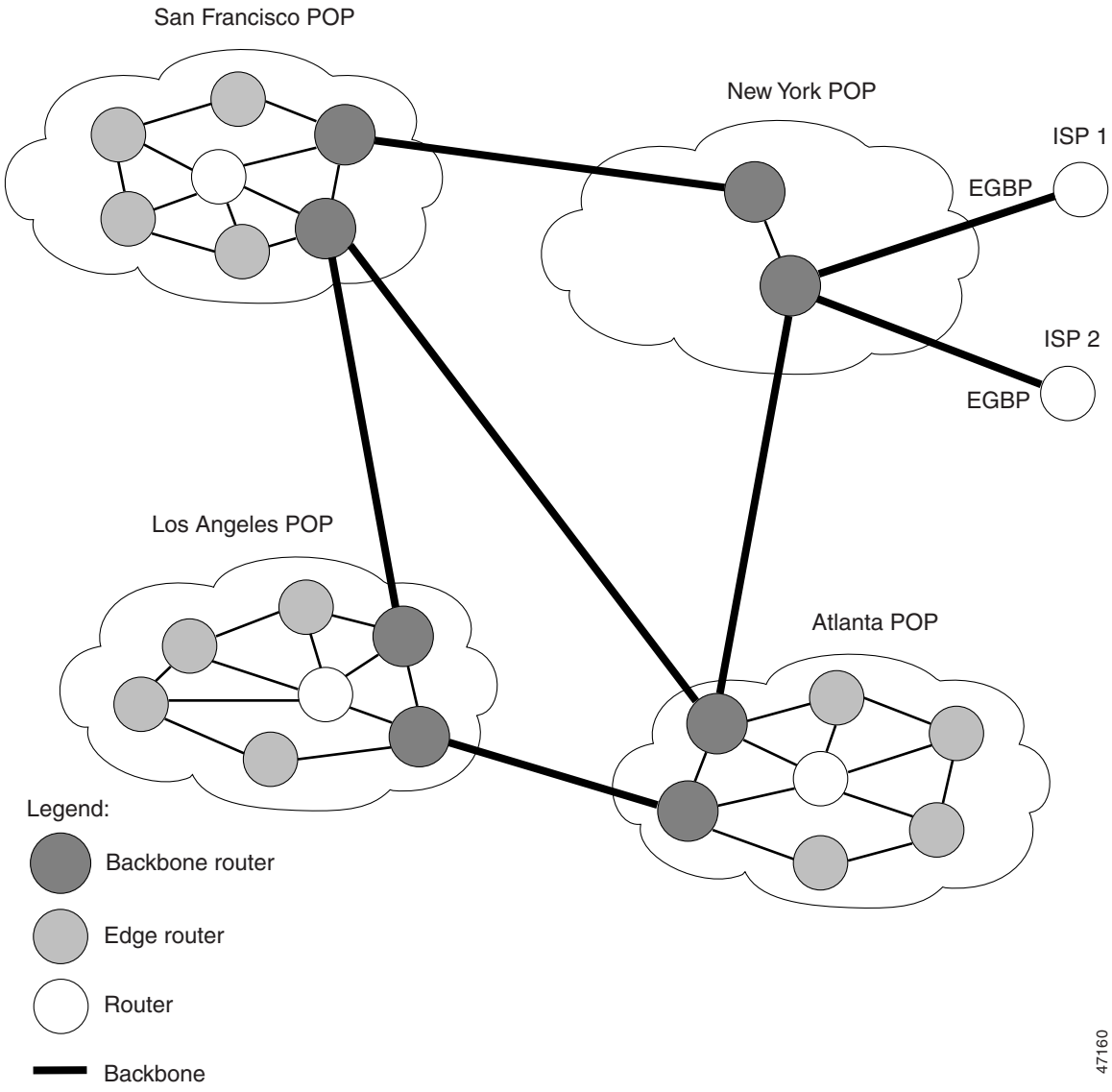
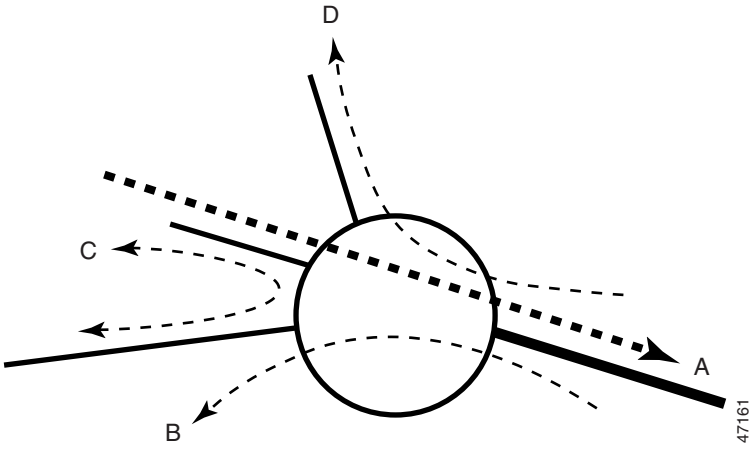


Figure 2 shows an exploded view of the backbone router that links the Los Angeles point of presence (POP) in Figure 1 to the Atlanta POP. The bold line represents the backbone link going to the Atlanta POP.

Figure 2 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.

Figure 2 Types of Traffic That Travel Through a Backbone Router



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 Figure 2) is the most important for determining the amount of traffic that travels through a backbone router. Internal traffic (paths B and D in Figure 2) 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:

- Viewing the data in a graphical format, using the NDA Display module. The Display module is useful for graphing the traffic matrix data and comparing statistics. See the “TMS Displayed with the NDA Display Module” section on page 7 for more information.

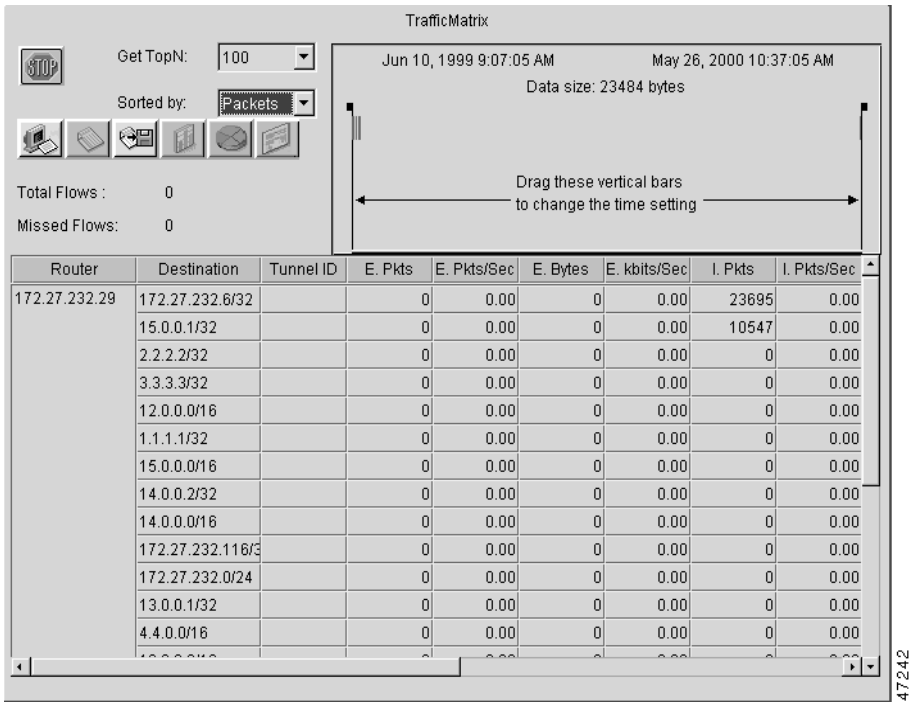
- Entering the **more system:vfiles/tmstats_ascii** command on the backbone router. This command displays a TMS table. See the "Interpreting the Statistics in the tmstats_ascii File" section on page 16 for more information.
- Entering the **show ip cef** command on the backbone router. This command displays nonrecursive accounting data for the backbone router. Included in the output are the numbers of packets and bytes of internal and external traffic that have been collected. See the "Nonrecursive Accounting Information Displayed with the show ip cef Command" section on page 8 for more information.

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 Figure 3 and Figure 4. The display format depends on the aggregation scheme you select. Refer to the *Network Data Analyzer Installation and User Guide* for more information.

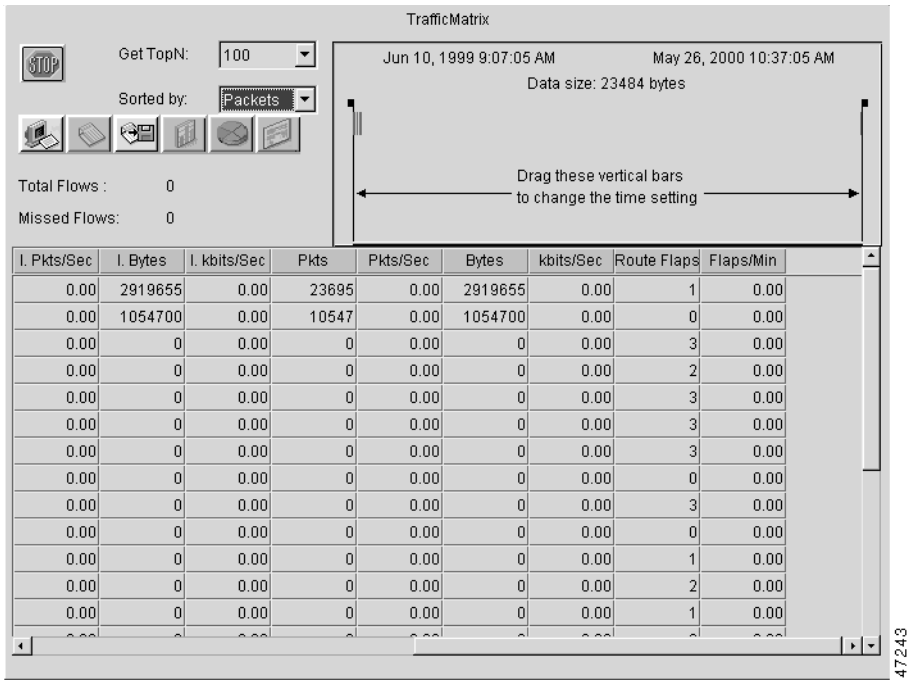
(The view of data that the NDA Display module provides is wide. Slide the scroll bar to the right and left to see all of the data. Figure 3 and Figure 4 taken together show all of the columns of data.)

Figure 3 Displaying TMS Through the NDA (Part 1)



Router	Destination	Tunnel ID	E. Pkts	E. Pkts/Sec	E. Bytes	E. kbits/Sec	I. Pkts	I. Pkts/Sec
172.27.232.29	172.27.232.6/32		0	0.00	0	0.00	23695	0.00
	15.0.0.1/32		0	0.00	0	0.00	10547	0.00
	2.2.2.2/32		0	0.00	0	0.00	0	0.00
	3.3.3.3/32		0	0.00	0	0.00	0	0.00
	12.0.0.0/16		0	0.00	0	0.00	0	0.00
	1.1.1.1/32		0	0.00	0	0.00	0	0.00
	15.0.0.0/16		0	0.00	0	0.00	0	0.00
	14.0.0.2/32		0	0.00	0	0.00	0	0.00
	14.0.0.0/16		0	0.00	0	0.00	0	0.00
	172.27.232.116/3		0	0.00	0	0.00	0	0.00
	172.27.232.0/24		0	0.00	0	0.00	0	0.00
	13.0.0.1/32		0	0.00	0	0.00	0	0.00
	4.4.0.0/16		0	0.00	0	0.00	0	0.00

Figure 4 Displaying TMS Through the NDA (Part 2)



I. Pkts/Sec	I. Bytes	I. kbits/Sec	Pkts	Pkts/Sec	Bytes	kbits/Sec	Route Flaps	Flaps/Min
0.00	2919655	0.00	23695	0.00	2919655	0.00	1	0.00
0.00	1054700	0.00	10547	0.00	1054700	0.00	0	0.00
0.00	0	0.00	0	0.00	0	0.00	3	0.00
0.00	0	0.00	0	0.00	0	0.00	2	0.00
0.00	0	0.00	0	0.00	0	0.00	3	0.00
0.00	0	0.00	0	0.00	0	0.00	3	0.00
0.00	0	0.00	0	0.00	0	0.00	3	0.00
0.00	0	0.00	0	0.00	0	0.00	0	0.00
0.00	0	0.00	0	0.00	0	0.00	3	0.00
0.00	0	0.00	0	0.00	0	0.00	0	0.00
0.00	0	0.00	0	0.00	0	0.00	1	0.00
0.00	0	0.00	0	0.00	0	0.00	2	0.00
0.00	0	0.00	0	0.00	0	0.00	1	0.00

Nonrecursive Accounting Information Displayed with the show ip cef Command

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, Ethernet0/0, 0 dependencies
  next hop 10.1.1.100, Ethernet0/0
  valid adjacency
  tag rewrite with Et0/0, 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
```

How to Configure Cisco Express Forwarding Network Accounting

Perform the following tasks to configure Cisco Express Forwarding network accounting:

- Configuring Cisco Express Forwarding Network Accounting, page 9 (required)
- Enabling a Backbone Router to Collect TMS, page 10 (optional)
- Interpreting the Statistics in the tmstats_ascii File, page 16 (optional)
- Viewing Information in the tmasinfo File: BGP Neighbor Autonomous Systems for IGP Destinations, page 19 (optional)
- Verifying Cisco Express Forwarding Network Accounting Information, page 21 (optional)

Configuring Cisco Express Forwarding 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`** **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	**ip cef accounting** {[**non-recursive**] [**per-prefix**] [**prefix-length**]} **Example:** `Router(config)# ip cef accounting per-prefix`	Enables Cisco Express Forwarding network accounting. • The **non-recursive** keyword enables you to count the number of packets and bytes express forwarded through nonrecursive prefixes. This keyword is optional when the command is used in global configuration mode. • The **per-prefix** keyword enables you to count the number of packets and bytes express forwarded to a destination IP address (or prefix). • The **prefix-length** keyword enables accounting based on prefix length.
Step 4	**exit** **Example:** `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, page 10 (optional)
- Enabling the NDA to Collect TMS on a Backbone Router, page 12 (optional)

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/port* or **interface** *type slot/port-adapter/port*

6. **ip cef accounting non-recursive** {**external** | **internal**}
7. **exit**
8. Repeat Steps 5, 6, and 7 for each incoming interface that you want to configure for TMS.

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	**ip cef** **Example:** `Router(config)# ip cef`	Enables Cisco Express Forwarding on the route processor card.
Step 4	**ip cef accounting** {[**non-recursive** [**per-prefix**] [**prefix-length**]} **Example:** `Router(config)# ip cef accounting non-recursive`	Enables Cisco Express Forwarding network accounting. • The **non-recursive** keyword enables you to count the number of packets and bytes express forwarded through nonrecursive prefixes. This keyword is optional when the command is used in global configuration mode. • The **per-prefix** keyword enables you to count the number of packets and bytes express forwarded to a destination (or prefix). • The **prefix-length** keyword enables accounting based on prefix length.

	Command or Action	Purpose

Step 5	**interface** type slot/port
	or
	interface type slot/port-adapter/port
	
	Example:
	`Router(config)# interface ethernet 1/1`
	
	or
	
	Example:
	`Router(config)# interface fastethernet 1/0/0`
		Configures an interface type and enters interface configuration mode.
		• The *type* argument specifies the type of interface to be configured.
		• The *slot/* argument specifies the slot number. Refer to the appropriate hardware manual for slot and port information.
		• The *port* argument specifies the port number. Refer to the appropriate hardware manual for slot and port information.
		• The *port-adapter/* argument specifies the port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.
		This command specifies the interface on the backbone router that you intend to configure.

Step 6	**ip cef accounting non-recursive** {**external** | **internal**} **Example:** `Router(config-if)# ip cef accounting non-recursive external`	Enables nonrecursive accounting on the router. • The **external** keyword calls for a count of input traffic data in the nonrecursive external bin. That is, this keyword sets the specified incoming interface so that it can collect data on traffic entering the backbone router from external sources. • The **internal** keyword calls for a count of input traffic data in the nonrecursive internal bin. That is, this keyword sets the specified incoming interface so that it can collect data on internal traffic in the backbone router.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits to privileged EXEC mode.
Step 8	Repeat Steps 5, 6, and 7 for each incoming interface that you want to configure for TMS.	—

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 Utility Server host in the network, the Traffic Matrix Statistics Control window shown in Figure 5 appears.

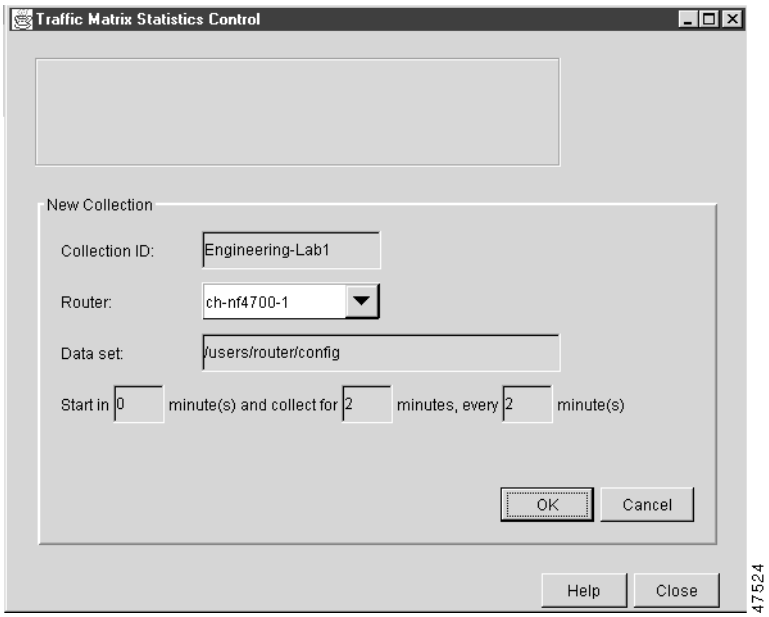
Step 3 Specify the new TMS collection parameters, using the Traffic Matrix Statistics Control window.

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 Figure 5.

Figure 5 Setting the NDA Traffic Matrix Statistics Control Window Collection Parameters



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 Figure 6 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 Figure 6.

Figure 6 Setting the NDA Configuration Window

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 Statistics in the tmstats_ascii File

This section contains information about and instructions for interpreting the statistics in the timstats_ascii file.

Before you perform the task to interpret the statistics in the tmstats_ascii file, you need to understand the following:

- Virtual Files on the Backbone Router, page 16
- tmstats_ascii File Header Description, page 16
- Destination Prefix Record Description, page 17
- Tunnel Midpoint Record Description, page 18

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_ascii 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>|AGGREGATIONTrafficMatrix.ascii|SYSUPTIME<seconds>|
routerUTC<routerUTC>|NTP<synchronized|unsynchronized>|DURATION<aggregateTime>|
```

Table 1 describes the fields in the file header of the tmstats_ascii file.

Table 1 Fields in tmstats_ascii File Header

Maximum Field Length	Field	Description
10	VERSION	File format version
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

Table 1 Fields in tmstats_ascii File Header (continued)

Maximum Field Length	Field	Description
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.

What are other record types?

Table 2 describes the fields in the destination prefix record.

Table 2 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. **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.
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>
```

Table 3 describes the fields in the tunnel midpoint record.

Table 3 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 |).

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:

```
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:

- Header information—"tmstats_ascii File Header Description" section on page 16

- Destination prefix record (dynamic label switching or traffic engineering (TE) tunnel data)—"Destination Prefix Record Description" section on page 17
- Tunnel midpoint record (TE tunnel midpoint data)—"Tunnel Midpoint Record Description" section on page 18

Viewing Information in the tmasinfo File: BGP Neighbor Autonomous Systems for IGP Destinations

Perform the following task to view information in the tmasinfo 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.

Before you view the statistics in the tmsasinfo file, you need to understand the following:

- Header Format for tmsasinfo File, page 19
- Neighbor AS Record in tmsasinfo File, page 20

Header Format for 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>|
```

Table 4 describes the fields in the file header.

Table 4 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 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>*

Table 5 describes the fields in the neighbor AS record.

Table 5 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)

SUMMARY STEPS

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

```
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:

- Header information—"Header Format for tmsasinfo File" section on page 19.
- Neighbor AS Record—"Neighbor AS Record in tmsasinfo File" section on page 20. The file displays BGP ASs associated with each IGP destination.

Verifying Cisco Express Forwarding Network Accounting Information

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

SUMMARY STEPS

1. **show ip cef summary**
2. **show ip cef** *interface-type number* **detail**

DETAILED STEPS

Step 1 **show ip cef summary**

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

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

```
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 2 **show ip cef** *interface-type 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 Ethernet 0. It shows all the prefixes resolving through adjacency pointing to next hop interface Ethernet 0/0 and next hop interface IP address 172.29.233.33.

For example, for Ethernet interface 0, IP address 172.29.233.33:

```
Router# show ip cef ethernet 0/0 detail

IP Distributed CEF with switching (Table Version 136808)

 45800 routes, 8 unresolved routes (0 old, 8 new)
 45800 leaves, 2868 nodes, 8444360 bytes,
 136808 inserts, 91008 invalidations
 1 load sharing elements, 208 bytes, 1 references
 1 CEF resets, 1 revisions of existing leaves
 refcounts: 527343 leaf, 465638 node

 172.29.233.33/32, version 7417, cached adjacency 172.29.233.33
 0 packets, 0 bytes,
   Adjacency-prefix
   via 172.29.233.33, Ethernet0/0, 0 dependencies

 next hop 172.29.233.33, Ethernet0/0
   valid cached adjacency
 0 packets, 0 bytes switched through the prefix
 tmstats: external 0 packets, 0 bytes
      internal 0 packets, 0 bytes
```

Configuration Examples for Configuring Cisco Express Forwarding Network Accounting

The following sections contain configuration examples for Cisco Express Forwarding accounting:

- Configuring Cisco Express Forwarding Network Accounting: Example, page 22
- Enabling a Backbone Router to Collect TMS Data: Example, page 23
- IP Cisco Express Forwarding Nonrecursive Accounting Configuration: Example, page 23
- Interpreting the Statistics in the tmstats_ascii File: Example, page 24

Configuring Cisco Express Forwarding Network Accounting: Example

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

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

Enabling a Backbone Router to Collect TMS Data: Example

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

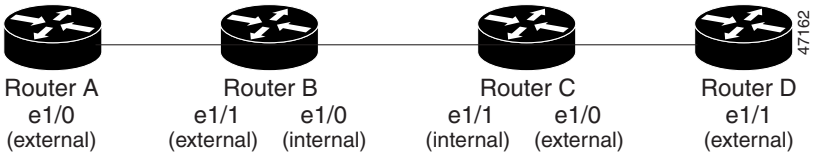
```
configure terminal
!
ip cef

ip cef accounting non-recursive
!
interface e1/0
 ip cef accounting non-recursive external
 end
```

For a sample backbone configuration, see the "IP Cisco Express Forwarding Nonrecursive Accounting Configuration: Example" section.

IP Cisco Express Forwarding Nonrecursive Accounting Configuration: Example

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. Figure 7 shows the sample backbone configuration.

Figure 7 Sample Backbone Configuration



Router A Configuration

```
Router(config)# ip cef
Router(config)# ip cef accounting non-recursive
Router(config)# interface e1/0
Router(config-if)# ip cef accounting non-recursive external
```

Router B Configuration: e1/1

```
Router(config)# ip cef
Router(config)# ip cef accounting non-recursive
Router(config)# interface e1/1
Router(config-if)# ip cef accounting non-recursive external
```

Router B Configuration: e1/0

```
Router(config)# interface e1/0
Router(config-if)# ip cef accounting non-recursive internal
```

Router C Configuration: e1/1:

```
Router(config)# ip cef
Router(config)# ip cef accounting non-recursive
Router(config)# interface e1/1
Router(config-if)# ip cef accounting non-recursive internal
```

Router C Configuration: e1/0

```
Router(config)# interface e1/0
```

```
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 e1/1
Router(config-if)# ip cef accounting non-recursive external
```

Interpreting the Statistics in the tmstats_ascii File: Example

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

The following sections provide references related to configuring network accounting for Cisco Express Forwarding.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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 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
Tasks for customizing the display of recorded Cisco Express Forwarding events	*Customizing the Display of Recorded Cisco Express Forwarding Events*
How to determine which Cisco IOS switching or forwarding path your packets are taking	*How to Verify Cisco Express Forwarding Switching*
How to use the Cisco Network Data Analyzer to view TMS	*Network Data Analyzer Installation and User Guide*
Commands for configuring and monitoring Cisco Express Forwarding	*Cisco IOS IP Switching Command Reference*

Standards

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Cisco Express Forwarding Network Accounting

Table 6 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

Table 6 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 Release 12.2(1) or later.	—	—

Glossary

AS—autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

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.

BGP—Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.

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 type of Cisco Express Forwarding switching 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. 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.

IGP— Interior Gateway Protocol. An internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

label—A short fixed-length data construct that tells switching nodes how to forward data (packets or cells).

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.

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.

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.

TE—traffic engineering. Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

traffic engineering tunnel—A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

TMS—Traffic Matrix Statistics. An IOS feature that enables an administrator to capture and analyze traffic data entering a backbone that is running the Border Gateway Protocol (BGP). This feature also allows an administrator to determine the neighbor autonomous systems of a BGP destination

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005—2008 Cisco Systems, Inc. All rights reserved.

Customizing the Display of Recorded Cisco Express Forwarding Events

First Published: May 2, 2005
Last Updated: February 11, 2008

This module contains information about and instructions for customizing the display of recorded Cisco Express Forwarding events for Cisco IOS releases prior to 12.2(25)S, 12.2(33)SB, 12.2(33)SRA, 12.2.(33)SXH, and 12.4(20)T.

For information about and instructions for customizing the display of recorded Cisco Express Forwarding events for Cisco IOS Releases 12.2(25)S, 12.2(33)SB, 12.2(33)SRA, 12.2.(33)SXH, 12.4(20)T, and later releases, see *Customizing the Display of Cisco IOS Event Trace Messages*.

You can customize the Cisco Express Forwarding event log display by specifying the size of the Cisco Express Forwarding event log or by choosing to display events by prefix and mask or by Cisco Express Forwarding Virtual Private Network (VPN) routing/forwarding instance (VRF).

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 feature information and caveats, see 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 for Configuring the Display of Recorded Cisco Express Forwarding Events" section on page 9.

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.

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

Contents

Prerequisites for Configuring the Display of Recorded Cisco Express Forwarding Events

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

Restrictions for Configuring the Display of Recorded Cisco Express Forwarding Events

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

Information About Configuring the Display of Recorded Cisco Express Forwarding Events

Before customizing Cisco Express Forwarding event logging, you should understand the following concepts:

- Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 3
- Cisco Express Forwarding Event Log Overview, page 3

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features that you can configure, go to the "Additional References" section on page 7.

Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding

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.

Cisco Express Forwarding Event Log Overview

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

When the Cisco Express Forwarding event log has reached its capacity, the oldest event is written over by the newest event. You can use the following commands to change the capacity of the Cisco Express Forwarding event log:

- The **ip cef table event-log** command allows you to increase or decrease the number of entries that the event log can hold.
- The **clear ip cef event-log** command allows you to clear all event log entries.

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

- The **show ip cef events** command displays all recorded Cisco Express Forwarding forwarding information base (FIB) and adjacency events.
- 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.

How to Customize the Display of Recorded Cisco Express Forwarding Events

Perform the following tasks to customize Cisco Express Forwarding event logging and display logging events:

- Customizing Cisco Express Forwarding Event Logging, page 4 (optional)
- Displaying Cisco Express Forwarding Event-Log Information, page 5 (optional)

Customizing Cisco Express Forwarding Event Logging

This section contains information about and instructions for customizing Cisco Express Forwarding event logging.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef table event-log** [**size** *event-number*] [**match** *ip-prefix mask*] [**vrf** *vrf-name*]
4. **exit**

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	**ip cef table event-log** [**size** *event-number*] [**match** *ip-prefix mask*] [**vrf** *vrf-name*] **Example:** `Router(config)# ip cef table event-log size 25000`	Controls Cisco Express Forwarding table event-log characteristics. • The **size** *event-number* keyword-argument pair specifies the number of event entries. The range is from 1 to 4294967295. • The **match** keyword logs events that match the specified prefix and mask. • The *ip-prefix* argument is the specified IP prefix to match in dotted decimal format (A.B.C.D). • The *mask* argument is the network mask written as A.B.C.D. • The **vrf** *vrf-name* keyword-argument pair displays the named Virtual Private Network (VPN) routing/forwarding instance (VRF) Cisco Express Forwarding table.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

Displaying Cisco Express Forwarding Event-Log Information

Perform the following task to display Cisco Express Forwarding event-log information.

SUMMARY STEPS

1. **enable**
2. **clear ip cef event-log**
3. **debug ip cef table**
4. **show ip cef events summary**
5. **show ip cef events within** *seconds*
6. **exit**

DETAILED STEPS

Step 1 **enable**

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

```
Router> enable
```

Enter your password if prompted.

Step 2 **clear ip cef event-log**

Use this command to clear the Cisco Express Forwarding event-log buffer. For example:

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

Step 3 **debug ip cef table**

Use this command to enable the collection of events that affect entries in the Cisco Express Forwarding tables. For 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 ip cef events summary**

Use this command to display a summary of recorded Cisco Express Forwarding FIB and adjacency events. For example:

```
Router# show ip cef events summary

CEF table events summary:
     Storage for 10000 events (320000 bytes), 822/0 events recorded/ignored
     Matching all events, traceback depth 16
     Last event occurred 00:00:06.516 ago.
```

Step 5 **show ip cef events within** *seconds*

Use this command to display Cisco Express Forwarding events that occurred within (during) a specified number of seconds. For example, within 1 second:

```
Router# show ip cef events within 1

CEF table events (storage for 10000 events, 14 events recorded)
+00:00:00.000:[Default-table] *.*.*.*/*           New FIB table          [OK]
+00:00:00.000:[Default-table] 10.1.80.194/32      FIB insert in mtrie    [OK]
+00:00:00.000:[Default-table] 10.1.80.0/32        FIB insert in mtrie    [OK]
+00:00:00.000:[Default-table] 10.1.80.255/32      FIB insert in mtrie    [OK]
+00:00:00.004:[Default-table] 10.1.80.0/24        FIB insert in mtrie    [OK]
+00:00:00.004:[Default-table] 10.1.80.0/24        NBD up                 [OK]
+00:00:00.004:[Default-table] 239.224.0.0/4       FIB insert in mtrie    [OK]
+00:00:00.012:[Default-table] 10.1.80.0/24        NBD up                 [Ignr]
+00:00:00.012:[Default-table] 239.224.0.0/4       FIB remove             [OK]
+00:00:00.016:[Default-table] 239.224.0.0/4       FIB insert in mtrie    [OK]
+00:00:05.012:[Default-table] 239.224.0.0/4       FIB remove             [OK]
+00:00:05.012:[Default-table] 239.224.0.0/4       FIB insert in mtrie    [OK]
+00:00:28.440:[Default-table] 239.224.0.0/4       FIB remove             [OK]
+00:00:28.440:[Default-table] 239.224.0.0/4       FIB insert in mtrie    [OK]
First event occured at 00:00:36.568 (00:04:40.756 ago)
Last event occured at 00:01:05.008 (00:04:12.316 ago)
```

Step 6 **exit**

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

```
Router# exit
Router>
```

Configuration Examples for Configuring the Display of Recorded Cisco Express Forwarding Events

This section contains one configuration example for customizing the display of recorded Cisco Express Forwarding events:

- Customizing Cisco Express Forwarding Event Logging: Example, page 7

Customizing Cisco Express Forwarding Event Logging: Example

The following example shows how to enable event logging for Cisco Express Forwarding:

```
clear ip cef event-log
!
debug ip cef table
!
configure terminal
!
ip cef table event-log size 25000
exit
!
```

In this example, the Cisco Express Forwarding event log is configured to hold 25000 entries.

Additional References

The following sections provide references related to the customizing of the display of recorded Cisco Express Forwarding events.

Related Documents

Related Topic	Document Title
Cisco Express Forwarding commands	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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 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
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 trace messages for Cisco IOS Releases 12.2(25)S, 12.2(33)SB, 12.2(33)SRA, 12.2.(33)SXH, 12.4(20)T and later releases	*Customizing the Display of Cisco IOS Event Trace Messages*
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*

Standards

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring the Display of Recorded Cisco Express Forwarding Events

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

Table 1 Feature Information for Configuring the Display of Recorded Cisco Express Forwarding Events

Feature Name	Releases	Feature Configuration Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS Release 12.2(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 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.

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.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)

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.

© 2005—2009 Cisco Systems, Inc. All rights reserved.

Customizing the Display of Cisco Express Forwarding Event Trace Messages

First Published: July 31, 2005
Last Updated: February 11, 2008

This module contains information about and instructions for customizing the display of recorded Cisco Express Forwarding events for Cisco IOS Releases 12.2(25)S, 12.2(33)SB, 12.2(33)SRA, 12.2.(33)SXH, 12.4(20)T, and later releases.

For information about and instructions for customizing the display of recorded Cisco Express Forwarding events for Cisco IOS releases prior to 12.2(25)S, 12.2(33)SB, 12.2(33)SRA, 12.2.(33)SXH, and 12.4(20)T, see *Customizing the Display of 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 feature information and caveats, see 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 for Configuring the Display of Cisco Express Forwarding Event Trace Messages" section on page 21.

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.

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

Contents

Prerequisites for Configuring the Display of Cisco Express Forwarding 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 Configuring the Display of Cisco Express Forwarding 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 fast switched. Logging disables Cisco Express Forwarding.

Information About Configuring the Display of Cisco Express Forwarding Event Trace Messages

Before customizing Cisco Express Forwarding event logging, you should understand the following concepts:

- Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding, page 3
- Overview of Cisco Express Forwarding Event Trace Function, page 3

For links to information about other Cisco Express Forwarding and distributed Cisco Express Forwarding features that you can configure, go to the "Additional References" section on page 19.

Cisco Platform Support for Central Cisco Express Forwarding and Distributed Cisco Express Forwarding

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.

Overview of Cisco Express Forwarding 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.

How to Customize the Display of Cisco Express Forwarding Event Trace Messages

Perform the following tasks to customize Cisco Express Forwarding event trace messaging and display event trace messages:

- Customizing Cisco Express Forwarding Event Tracing, page 4 (optional)
- Customizing Cisco Express Forwarding Event Tracing for IPv4 Events, page 8 (optional)
- Customizing Cisco Express Forwarding Event Tracing for IPv6 Events, page 10 (optional)
- Displaying Cisco Express Forwarding Event Trace Information, page 13 (optional)

Customizing Cisco Express Forwarding 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.

Cisco Express Forwarding 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.

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`** **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	**monitor event-trace cef** {**dump-file** *dump-file-name* | {**events** | **interface**} {**disable** | **dump-file** *dump-file-name* | **enable** | **size** *number* | **stacktrace** [*depth*]}} **Example:** `Router(config)# monitor event-trace cef dump-file tftp://172.16.10.5/cef-events`	Configures event tracing for Cisco Express Forwarding. • 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. • The **events** keyword turns on event tracing for Cisco Express Forwarding events. • The **interface** keyword turns on event tracing for Cisco Express Forwarding interface events. • The **disable** keyword turns off event tracing for Cisco Express Forwarding events. • 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. • 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. **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. • The **stacktrace** keyword enables the stack trace at tracepoints. • The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**monitor event-trace cef** {**dump** [**merged pretty** | **pretty**] | {**events** | **interface** | **ipv4** | **ipv6**} {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}} **Example:** `Router# monitor event-trace cef events dump pretty`	Monitors and controls the event trace function for Cisco Express Forwarding. • 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. • The **merged pretty** keywords sort all event trace entries by time and write the entries to a file in ASCII format. • The **pretty** keyword saves the event trace message in ASCII format. • The **events** keyword monitors Cisco Express Forwarding events. • The **interface** keyword monitors Cisco Express Forwarding interface events. • The **ipv4** keyword monitors Cisco Express Forwarding IPv4 events. • The **ipv6** keyword monitors Cisco Express Forwarding IPv6 events. • The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device. • The **continuous** keyword continuously displays the latest event trace entries. • The **cancel** keyword cancels the continuous display of the latest trace entries. • The **disable** keyword turns off Cisco Express Forwarding event tracing. • The **enable** keyword turns on Cisco Express Forwarding event tracing. • 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** **Example:** `Router# disable`	Exits to user EXEC mode.

Customizing Cisco Express Forwarding 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.

Cisco Express Forwarding Event Tracing for IPv4 Events Defaults and Options

Event tracing for Cisco Express Forwarding IPv4 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 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.

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`** **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	**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*}]} **Example:** `Router(config)# monitor event-trace cef ipv4 size 10000`	Configures event-tracing for Cisco Express Forwarding IPv4 events. • The **disable** keyword turns off event tracing for Cisco Express Forwarding IPv4 events. • The **distribution** keyword logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards • 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. • 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. • 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 • The **global** keyword specifies global events. • The *ip-address mask* arguments specify an IP address in A.B.C.D format and a subnet mask in A.B.C.D format. • 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. **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. • The **stacktrace** keyword enables the stack trace at tracepoints. • The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16. • 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** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**monitor event-trace cef ipv4** {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**} **Example:** `Router# monitor event-trace cef ipv4 continuous`	Monitors and controls the event trace function for Cisco Express Forwarding IPv4 events. • The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device. • The **continuous** keyword continuously displays the latest event trace entries. • The **cancel** keyword cancels the continuous display of the latest trace entries. • The **disable** keyword turns off Cisco Express Forwarding event tracing. • 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. • The **pretty** keyword saves the event trace message in ASCII format. • The **enable** keyword turns on Cisco Express Forwarding event tracing. • 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** **Example:** `Router# disable`	Exits to user EXEC mode.

Customizing Cisco Express Forwarding 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.

Cisco Express Forwarding Event Tracing for IPv6 Events Defaults and Options

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace cef ipv6** {**disable** | **distribution** | **dump-file** *dump-file-name* | **enable** | **match** {**global** | *ipv6-address/n* | **size** *number* | **stacktrace** [*depth*] | **vrf** *vrf-name* [**distribution** | **match** {**global** | *ipv6-address/n*}]}
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`** **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	**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*}]} **Example:** `Router(config)# monitor event-trace cef ipv6 match global`	Configures event-tracing for Cisco Express Forwarding IPv6 events. • The **disable** keyword turns off event tracing for Cisco Express Forwarding IPv6 events. • The **distribution** keyword logs events related to the distribution of Cisco Express Forwarding FIB tables to the line cards. • 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. • 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. • 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. • The **global** keyword specifies global events. • 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 • 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. **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. • The **stacktrace** keyword enables the stack trace at tracepoints. • The *depth* argument specifies the depth of the stack trace stored. Range: 1 to 16. • 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

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.
Step 5	**monitor event-trace cef ipv6** {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}} **Example:** `Router# monitor event-trace cef ipv6 one-shot`	Monitors and controls the event trace function for Cisco Express Forwarding IPv6 events. • The **clear** keyword clears existing trace messages for Cisco Express Forwarding from memory on the networking device. • The **continuous** keyword continuously displays the latest event trace entries. • The **cancel** keyword cancels the continuous display of the latest trace entries. • The **disable** keyword turns off Cisco Express Forwarding event tracing. • 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. • The **pretty** keyword saves the event trace message in ASCII format. • The **enable** keyword turns on Cisco Express Forwarding event tracing. • 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** **Example:** `Router# disable`	Exits to privileged EXEC mode.

Displaying Cisco Express Forwarding 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 event-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:

```
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
```

Step 3 **debug ip cef table**

Use this command to display events that affect entries in the Cisco Express Forwarding tables. For 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:

```
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:

```
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:

```
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:

```
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:

```
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:

```
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:

```
Router# disable
Router>
```

Configuration Examples for Configuring the Display of Cisco Express Forwarding Event Trace Messages

This section contains the following configuration examples for customizing the display of recorded Cisco Express Forwarding events:

- Customizing Cisco Express Forwarding Event Tracing: Examples, page 17
- Customizing Cisco Express Forwarding Event Tracing for IPv4 Events: Examples, page 18
- Customizing Cisco Express Forwarding Event Tracing for IPv6 Events: Examples, page 19

Customizing Cisco Express Forwarding 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
```

Customizing Cisco Express Forwarding Event Tracing for IPv4 Events: Examples

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
```

Customizing Cisco Express Forwarding Event Tracing for IPv6 Events: Examples

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

The following sections provide references related to the customizing of the display of recorded Cisco Express Forwarding events.

Related Documents

Related Topic	Document Title
Cisco Express Forwarding commands	*Cisco IOS IP Switching Command Reference*
List of the features documented in the Cisco Express Forwarding modules	*Cisco Express Forwarding Features Roadmap*
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 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*
Tasks for customizing the display of recorded Cisco Express Forwarding events in Cisco IOS releases prior to Cisco IOS Releases 12.2(25)S, 12.2(33)SB, 12.2(33)SRA, 12.2(33)SXH, and 12.4(20)T	*Customizing the Display of Recorded Cisco Express Forwarding Events*
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*

Standards

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

MIBs

MIBs	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

RFCs	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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring the Display of Cisco Express Forwarding Event Trace Messages

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the *Cisco Express Forwarding Features Roadmap*.

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

Table 1 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 Release 12.2(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 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.

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.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.

Cisco Express Forwarding—SNMP CEF-MIB Support

First Published: December 4, 2006
Last Updated: November 25, 2009

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 feature information and caveats, see 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 for Cisco Express Forwarding—SNMP CEF-MIB Support" section on page 30.

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

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

Prerequisites for Cisco Express Forwarding—SNMP CEF-MIB Support

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

- Cisco Express Forwarding or distributed Cisco Express Forwarding must be configured on your system.
- The Cisco Express Forwarding infrastructure introduced in Cisco IOS Release12.2(25)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 must be configured for SNMP access. See the "Configuring the Router to Use SNMP" section on page 15 of this document for more information.

Information About Cisco Express Forwarding—SNMP CEF-MIB Support

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

Cisco Express Forwarding 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.

In Cisco IOS Release 12.2(31)SB and later releases, 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 Release 12.2(22)S.

The implementation of the CISCO-CEF-MIB in Cisco IOS Release 12.2(31)SB2, Cisco IOS Release 12.2(33)SRC,and Cisco IOS Release 12.2(33)SB 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).

Cisco Express Forwarding 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 and Related Tables

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.

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:

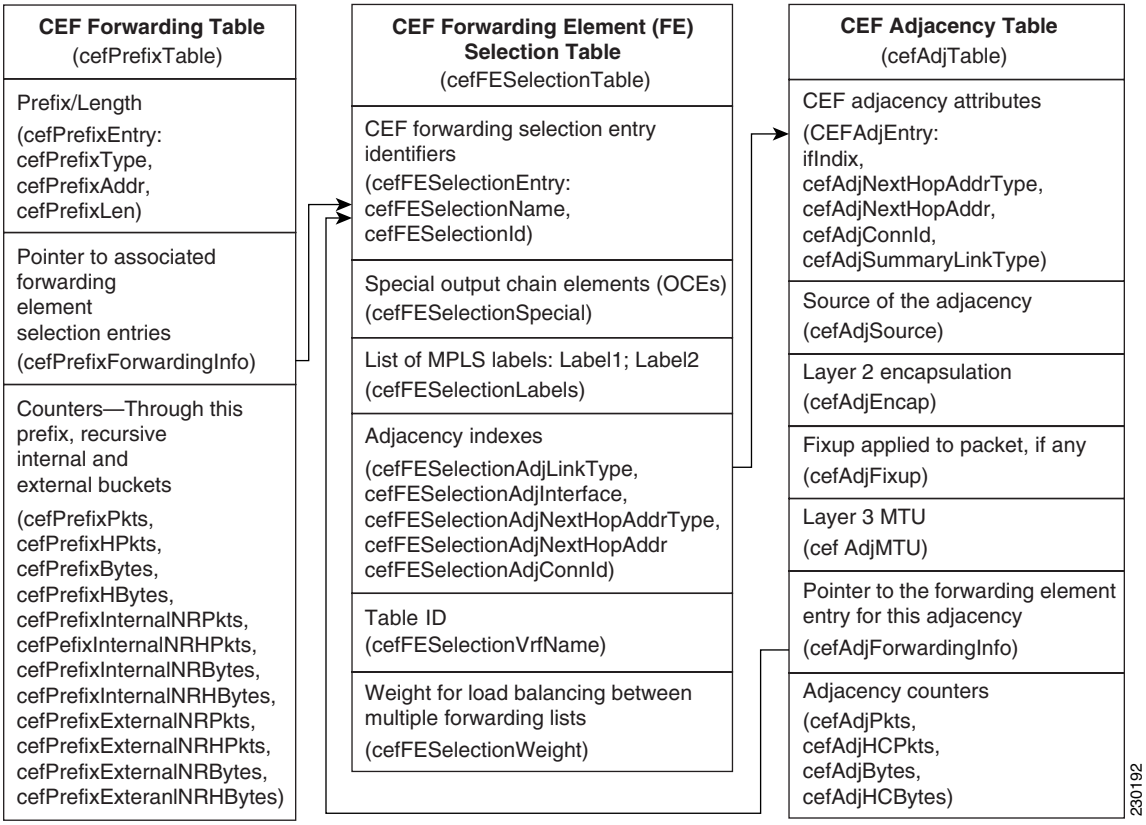
- The CEF FIB Summary table (cefFIBSummaryTable) contains the number of forwarding prefixes for both IPv4 and IPv6 protocols. It is a summary of the CEF Forwarding table.
- The CEF Forwarding table (cefPrefixTable) lists all the prefixes and related counters. It also contains a pointer to the CEF Forwarding 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 the"Cisco Express Forwarding 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 main tables and the relationships of the tables to one another.

Figure 1 CISCO-CEF-MIB Main Tables, Table Contents, and Relationships



Cisco Express Forwarding Configuration and Monitoring 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.

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

Table 1 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**

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

Table 2 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
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

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

Table 3 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

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

Table 4 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

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

Table 5 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

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

Table 6 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

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

Table 7 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

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

Table 8 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 • nonRecursive (0) • perPrefix (1) • prefixLength (2)
Gets or sets Cisco Express Forwarding 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 Cisco Express Forwarding 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 Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Resource table (cefResourceTable).

Table 9 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

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

Table 10 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 • cefEnabled (1) • distCefEnabled (2) • cefDisabled (3)
Gets or sets the type of Cisco Express Forwarding Load sharing on the interface	cefIntLoadSharing • perPacket (1) • perDestination (2)
Gets or sets Cisco Express Forwarding nonrecursive accounting on the interface	cefIntNonrecursiveAccouting • internal (1) • external (2)

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

Table 11 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

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

Table 12 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

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

Table 13 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

Table 13 CEF Prefix Length Statistics Table—Cisco Express Forwarding Operations and Associated MIB Objects (continued)

Cisco Express Forwarding Operation	MIB Object
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 Cisco Express Forwarding monitoring operations and associated MIB objects provided by the CEF Switching Statistics table (cefSwitchingStatsTable).

Table 14 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
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

Table 15 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 15 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

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

Table 16 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

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

Table 17 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

Table 17 CEF Inconsistency Record Table—Cisco Express Forwarding Operations and Associated MIB Objects (continued)

Cisco Express Forwarding Operation	MIB Objects
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 Cisco Express Forwarding 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 Cisco Express Forwarding operations associated with the CISCO-CEF-MIB objects that enable the sending of Cisco Express Forwarding notifications.

Table 18 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. 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
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** 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** 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** 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** 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 Notifications, page 24 (optional)

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** **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* [**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 that are 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 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.

	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 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** **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-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** **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 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).

	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 User Datagram Protocol (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.

Configuring SNMP Notifications for Cisco Express Forwarding Events

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

Prerequisites

You must have configured 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.

	Command or Action	Purpose
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 Cisco Express Forwarding peers. • The **resource-failure** keyword enables the sending of CISCO-CEF-MIB SNMP notifications for resource failures that affect Cisco Express Forwarding 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 Notifications" 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 Cisco Express Forwarding 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 or informs. 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 Cisco Express Forwarding 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 Cisco Express Forwarding FIB on the RP and to the Cisco Express Forwarding 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 Notifications

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 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

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. A valid value is from 0 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. A valid value is from 0 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, page 26
- Configuring SNMP Notifications for Cisco Express Forwarding Events: Example, page 26
- Configuring the Throttling Interval for CISCO-CEF-MIB Inconsistency Notifications: Example, page 27

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 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
```

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

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

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

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
Overview of Cisco Express Forwarding, and links to related Cisco Express Forwarding documents	"Cisco Express Forwarding Overview" module

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 Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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

Table 20 lists the release history for this feature.

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 20 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 20 Feature Information for Cisco Express Forwarding—SNMP CEF-MIB Support

Feature Name	Release	Feature Information
Cisco Express Forwarding—SNMP CEF-MIB Support	12.2(31)SB2 12.2(33)SRC 12.2(33)SB 12.4(20)T 15.0(1)M 12.2(33)SRE	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. In 12.2(31)SB2, this feature was introduced on the Cisco 10000. In 12.2(33)SRC, this feature was integrated into a Cisco IOS 12.2SR release. In 12.2(33)SB, this feature was integrated into a Cisco IOS 12.2SB release. In 12.4(20)T, this feature was integrated into a Cisco IOS 12.4T release. In 15.0(1)M, this feature was integrated into a Cisco IOS 15.0(1)M release. In 12.2(33)SRE, this feature was integrated into a Cisco_IOS 12.2SRE release. The following sections provide information about this feature: • Cisco Express Forwarding Functional Overview, page 2 • Benefits of CISCO-CEF-MIB, page 3 • Cisco Express Forwarding 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 Configuration and Monitoring Operations Available Through the CISCO-CEF-MIB, page 6CISCO-CEF-MIB Notifications, page 14 • Configuring the Router to Use SNMP, page 15

Table 20 Feature Information for Cisco Express Forwarding—SNMP CEF-MIB Support (continued)

Feature Name	Release	Feature Information
		• 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 Notifications, page 24 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 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.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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 – 2009 Cisco Systems, Inc. All rights reserved.

Cisco Express Forwarding: Command Changes

First Published: August 11, 2004
Last Updated: July 11, 2008

This feature module details changes to commands that are required to support updates to Cisco Express Forwarding.

In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, and 12.4(20)T, Cisco Express Forwarding has been updated to support new features and new hardware. These updates enable Cisco Express Forwarding to operate with the Multiprotocol Label Switching (MPLS) High Availability (HA) applications and the MPLS Forwarding Infrastructure (MFI).

Cisco Express Forwarding provides a forwarding path and maintains a complete forwarding and adjacency table for both the software and hardware forwarding engines.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Cisco Express Forwarding: Command Changes" section on page 5.

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

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

Information About Cisco Express Forwarding: Command Changes

Before using the Cisco Express Forwarding commands, you should understand the following concepts:

- Deleted Commands, page 2
- Replaced Commands, page 3

Deleted Commands

The following commands are obsolete and are no longer available from Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and future releases (no replacement commands are provided):

- **clear adjacency epoch**
- **clear cef linecard events**
- **clear ip cef epoch**
- **clear ip cef events**
- **clear ip cef * prefix-statistics**
- **debug adjacency adjlist**
- **debug ip cef bulk-xfer**
- **debug ip cef elog-cef**
- **debug ip cef elog-plat**
- **debug ip cef stats**
- **ip cef switch**
- **ip cef linecard event-log**
- **ip cef linecard reloader**
- **ip cef load-sharing algorithm jittered**
- **ip cef nsf sync**
- **ip cef table event-log**
- **ip cef table resolution-timer**
- **ip cef table short-mask-protection**
- **show cef events**
- **show cef linecard events**

Replaced Commands

Table 1 lists all replaced Cisco Express Forwarding commands, starting with Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, and 12.4(20)T, for the Cisco 7500 series routers:

Table 1 Replaced Cisco Express Forwarding Commands—Cisco 7500 Series Routers

Command	Replacement Command
ip cef table consistency-check	**cef table consistency-check**
debug ip cef adjfib	**debug cef fib attached export**
ip cef switch	**ip cef**
clear ip cef event-log	**monitor event-trace cef ipv4 clear**
ip cef linecard event-log max-events	**monitor event-trace cef linecard size**
show adjacency nexthop	**show adjacency**
show cef drop	**show ip cef switching statistics**
show cef not-cef-switched	**show ip cef switching statistics**
show cef events	**show monitor event-trace**
show ip cef events (still visible)	**show monitor event-trace cef events**
show cef events [internal]	**show monitor event-trace cef events all**
show cef linecard events	**show monitor event-trace cef linecard**

Table 2 lists all replaced Cisco Express Forwarding commands, starting with Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, and 12.4(20)T for the Cisco 10000 series routers:

Table 2 Replaced Cisco Express Forwarding Commands—Cisco 10000 Series Routers

Command	Replacement Command
ip cef table consistency-check	**cef table consistency-check**
debug ip cef adjfib	**debug cef fib attached export**
clear ip cef event-log	**monitor event-trace cef ipv4 clear**
show adjacency nexthop	**show adjacency**
show cef drop	**show ip cef switching statistics**
show cef events	**show monitor event-trace**
show ip cef events (still visible)	**show monitor event-trace cef events**
show cef events [internal]	**show monitor event-trace cef events all**
show cef linecard events	–

Additional References

For additional information related to the Cisco Express Forwarding command changes, see the following references:

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
MPLS HA applications and MFI	*MPLS High Availability: Overview*

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco Express Forwarding: Command Changes

Table 3 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 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Cisco Express Forwarding: Command Changes

Feature Name	Releases	Feature Information
Cisco Express Forwarding: Command Changes	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH 12.4(20)T	In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, Cisco Express Forwarding has been updated to support new features and new hardware. These updates enable Cisco Express Forwarding to operate with the Multiprotocol Label Switching (MPLS) High Availability (HA) applications and the MPLS Forwarding Infrastructure (MFI). This feature module details changes to commands that are required to support updates to Cisco Express Forwarding. In 12.2(25)S, this feature was introduced and supported on the Cisco 7500 series routers. In 12.2(28)SB, this feature was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers. In 12.2(33)SRA, this feature was integrated into Cisco IOS Release 12.2(33)SRA. In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH. In 12.4(20)T, this feature was integrated into a Cisco IOS 12.4T release. The following sections provide information about this feature: • "Deleted Commands" section on page 2 • "Replaced Commands" section on page 3. The following commands were modified: **cef table consistency-check, clear adjacency, clear cef linecard, clear cef table, clear ip cef inconsistency, debug adjacency, debug cef, debug ip cef, debug ip cef accounting non-recursive, debug ip cef fragmentation, debug ip cef hash, debug ip cef subblock, debug ip cef table, ip route-cache, monitor event-trace (EXEC), monitor event-trace (global), show adjacency, show cef, show cef features global, show cef interface, show ip cef, show ip cef adjacency, show ip cef non-recursive, show ip cef switching statistics, show ip cef tree, show ip cef unresolved, show ip traffic, show monitor event-trace, show xdr.**

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2004 – 2008 Cisco Systems, Inc. All rights reserved.

Cisco Express Forwarding Enhancements: Removal of IP Fast Switching and Introduction of CLI Changes

First Published: July 11, 2008
Last Updated: July 11, 2008

The purpose of this document is to describe the changes based on the Cisco Express Forwarding infrastructure scalability enhancements that have been implemented to adapt to the evolution of the Internet and to support new platforms and features. The changes are the removal of IP fast switching and the introduction of command line interface (CLI) modifications.

This document lists Cisco Express Forwarding CLI commands that are removed, replaced, changed, and new. To help you transition to the new CLI format, the document illustrates the output for new commands and changed commands.

Enhancements to Cisco Express Forwarding enable it to operate with the Multiprotocol Label Switching (MPLS) Forwarding Infrastructure (MFI) and guarantee consistency across Cisco IOS release trains. Cisco Express Forwarding infrastructure changes were introduced and implemented in the Cisco IOS 12.2(25)S-based releases and were added for T releases in Cisco IOS Release 12.4(20)T.

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 feature information and caveats, see 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 for Cisco Express Forwarding" section on page 28.

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.

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

Contents

Information About Cisco Express Forwarding

This document presents the following topics to explain the changes you will find with the implementation of the Cisco Express Forwarding enhancements. This information should be helpful as you transition to Cisco IOS software that includes the Cisco Express Forwarding and MFI enhancements.

The fifth and sixth topics provide information about the CLI changes implemented as part of the Cisco Express Forwarding enhancements. In each section, the commands that are changed are listed, followed by an explanation of how they are changed. Sample command output is included in sections to compare “before” and “after” output information and to provide new output information.

The information about the commands is presented in the following order:

- Removed or existing, but unsupported, commands
- Commands with modified output
- New commands created for output consistency
- Related commands with unchanged output

Introduction of Cisco Express Forwarding Enhancements

Cisco Express Forwarding is at the heart of switching in every router. Improvements have been made to the Cisco Express Forwarding infrastructure to enhance and scale switching. Cisco Express Forwarding enhancements were introduced in Cisco IOS Release 12.2(25)S and first adopted by Cisco IOS 12.2(25)S-based releases. In Cisco IOS Release 12.4(20)T, the Cisco Express Forwarding enhancements were added for Cisco IOS 12.4(20)T releases and later T-based releases.

Table 1 lists the Cisco IOS releases and platforms that support the Cisco Express Forwarding enhancements and the changes described in this document.

Table 1 Cisco IOS Releases and Platforms That Support Cisco Express Forwarding Enhancements

Cisco IOS Release	Platforms Supported
12.2(25)SE	Catalyst 2970 series switches Catalyst 3500 series switches Catalyst 3750 series switches
12.2(25)SG	Catalyst 4500 series Switches
12.2(28)SB	Cisco 7200 series routers Cisco 7301 series routers Cisco 7304 series routers Cisco 10000 series routers
12.2(33)SRA	Cisco 7600 series routers
12.2(33)SXH	Catalyst 6500 series switches
12.4(20)T	Cisco 800 series routers Cisco 1700 series routers Cisco 1800 series routers Cisco 2600 series routers Cisco 2800 series routers Cisco 3200 series routers Cisco 3600 series routers Cisco 3700 series routers Cisco 3800 series routers Cisco 7200 series routers Cisco 7400 series routers Cisco 8850 series routers Cisco AS5000 series universal gateways

Cisco Express Forwarding Enhancements for Cisco IOS Release 12.4(20)T

Cisco IOS Release 12.4(20)T incorporates the following Cisco Express Forwarding infrastructure changes:

- Cisco Express Forwarding Scalability and Selective Rewrite (CSSR) for enhanced scalable, distributed Layer 3 switching
- Enhanced Multiprotocol Label Switching (MPLS) Forwarding Infrastructure (MFI)

  For information on MFI enhancements, see *MPLS Infrastructure Changes: Introduction of MFI and Removal of MPLS LSC and LC-ATM Features*.

The Cisco Express Forwarding infrastructure changes provide the following:

- Simplified fast switching path decisions for both IPv4 and IPv6 traffic, which improve performance and provide more CPU cycles for other Cisco IOS services
- Enhanced scalability to support large numbers of the following:
  - IPv4 and IPv6 prefixes and adjacencies
  - Load balancing paths over multiple links based on Layer 3 routing information
  - Virtual Private Network (VPN) routing and forwarding (VRF) instances

- Improved manageability of the following:
  - Cisco Express Forwarding logging for both IPv4 and IPv6
  - Unicast Reverse Path Forwarding (uRPF) strict and loose mode
  - Cisco Express Forwarding MIB (CEF-MIB)
  - uRPF MIB
  - CLI display enhancements for Cisco Express Forwarding

No new features are introduced in Cisco IOS Release 12.4(20)T. However, some features that previously shipped with a Cisco IOS 12.2(25)S-based release are new to the Cisco IOS 12.4T release.

Note CSSR and MFI enhancements in Cisco IOS Release 12.4(20)T might result in changed performance characteristics in your network. We suggest that you test configurations before upgrading to this software.

Removal of Support for IPv4 Fast Switching

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

Note Starting with the implementation of the Cisco Express Forwarding enhancements and the removal of IPv4 fast switching, components that do not support Cisco Express Forwarding will work only in process switched mode.

Removed, Obsolete, and No Longer Supported Cisco Express Forwarding Commands

The following commands are obsolete and have been removed from Cisco IOS software with the present Cisco Express Forwarding enhancements:

- **show ip cef inconsistency records**
- **show ip cef inconsistency now**
- **show ip cef inconsistency now detail**

Table 2 lists the commands that replace the removed commands.

Table 2 Removed Cisco Express Forwarding Commands—Cisco Express Forwarding

Command Before Cisco Express Forwarding Enhancements	Replacement Command After Cisco Express Forwarding Enhancements
ip cef table adjacency-prefix	—
ip cef table resolution-timer	—
show ip cef inconsistency records	**test cef table consistency**

Table 2 Removed Cisco Express Forwarding Commands—Cisco Express Forwarding (continued)

Command Before Cisco Express Forwarding Enhancements	Replacement Command After Cisco Express Forwarding Enhancements
show ip cef inconsistency now	**test cef table consistency**
show ip cef inconsistency now detail	**test cef table consistency detail**

The following commands still exist, but are no longer supported in Cisco IOS software:

- **show cef events**
- **show cef dropped**
- **show cef non-cef-switched**

Table 3 lists commands that still exist, but are no longer supported, and the commands that replaces the unsupported commands. You should start using the replacement commands.

Table 3 Replaced Cisco Express Forwarding Commands—Cisco Express Forwarding Feature

Command Before Cisco Express Forwarding Enhancements	Replacement Command After Cisco Express Forwarding Enhancements
ip cef event -log	**monitor event-log cef event**
ip cef interface event-log	**monitor event-log cef interface**
ip cef table event-log	**monitor event-log cef ipv4**
ip cef table consistency-check	**cef table consistency-check**
ip cef loadinfo	**cef table output-chain**
show cef events	**show monitor event-trace cef events all**
show cef drop	**show {ip | ipv6} cef switching statistics [feature]**[1]
show cef not-cef-switched	**show {ip | ipv6} cef switching statistics [feature]**

1. If you enter the optional **feature** keyword, the output shows per-feature drop and punt counters.

Cisco Express Forwarding CLI Command Output Changes

This section describes the CLI command output changes introduced with the Cisco Express Forwarding feature. In some commands the output format is changed. In other commands, pieces of information are added or removed from the output. The output of the following commands is changed with this feature:

- **show ip cef summary**
- **show ipv6 cef summary**
- **show ip cef internal**
- **show ipv6 cef internal**
- **show ip cef detail**
- **show ipv6 cef detail**
- **show ip cef <prefix> internal**
- **show ipv6 cef <prefix> internal**
- **show ip cef <prefix>**

- **show ip cef exact-route <source> <destination> detail**
- **show ip cef exact-route <source> <destination>**
- **show ip cef adjacency <interface> <next-hop>**
- **show adjacency summary**
- **show adjacency detail**
- **show adjacency internal**
- **show cef state**
- **show cef timers**
- **show ip cef epoch**
- **show ipv6 cef epoch**
- **show ip cef unresolved detail**
- **show ipv6 cef unresolved detail**
- **show ipv6 cef non-recursive**

For a full description of these commands, see the *Cisco IOS IP Switching Command Reference* and the *Cisco IOS IPv6 Command Reference*.

show ip cef summary

This feature provides the following changes to the output of the **show ip cef summary** command:

- IPv4 and IPv6 are separately addressed.
- Figures related to adjacencies are moved to the **show adjacency summary** command (see the "show adjacency summary" section on page 16).
- Mtrie data structure descriptions are moved to a new command, the **show ip cef tree** command (see the "New Commands for the Cisco Express Forwarding Feature" section on page 24).

Table 4 compares the **show ip cef summary** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 4 show ip cef summary Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

Router# **show ip cef summary**
 	
IP CEF with switching (Table Version 32), flags=0x0
  26 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
  26 leaves, 19 nodes, 23400 bytes, 53 inserts, 27 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id DF940F94
  3(0) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts: 1342 leaf, 1321 node
 	
  Table epoch: 0 (26 entries at this epoch)
 	
Adjacency Table has 4 adjacencies
  2 IPv4 adjacencies
  2 IPv6 adjacencies
	Router# **show ip cef summary**
	
	IPv4 CEF is enabled and running
	VRF Default:
	 22 prefixes (22/0 fwd/non-fwd)
	 Table id 0
	 Database epoch: 0 (22 entries at this epoch)

show ipv6 cef summary

This feature provides the following change to the output of the **show ipv6 cef summary** command:

- Output is reformatted (information provided is similar to what was provided before the Cisco Express Forwarding enhancement.)

Table 5 compares the **show ipv6 cef summary** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 5 show ipv6 cef summary Command Output Before and After Cisco Express Forwarding Enhancements

Old	New
Router# **show ipv6 cef summary** IPv6 CEF is enabled and running Slow processing intvl = 1 seconds backoff level current/max 0/0 0 unresolved prefixes, 0 requiring adjacency update IPv6 CEF default table 19 prefixes	Router# **show ipv6 cef summary** IPv6 CEF is enabled and running VRF Default: 20 prefixes (20/0 fwd/non-fwd) Table id 0 Database epoch: 0 (20 entries at this epoch)

show ip cef internal

This feature provides the following changes to the output of the **show ip cef internal** command:

- IPv4 and IPv6 are separately addressed.
- Mtrie data structure descriptions are moved to a new command, the **show ip cef tree** command (see the "New Commands for the Cisco Express Forwarding Feature" section on page 24).

- Troubleshooting is made easier with the addition of references to internal structure pointers.
- The concept of output chain (chain of output features) is introduced.

Table 6 compares the **show ip cef internal** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 6 show ip cef internal Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

Router# **show ip cef internal**
 	
IP CEF with switching (Table Version 32), flags=0x0
  26 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
  26 leaves, 19 nodes, 23400 bytes, 53 inserts, 27 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id DF940F94
  3(0) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts: 1342 leaf, 1321 node
 	
  Table epoch: 0 (26 entries at this epoch)
 	
Adjacency Table has 3 adjacencies
  1 IPv4 adjacency
  2 IPv6 adjacencies
0.0.0.0/32, version 0, epoch 0, receive
10.10.1.1/32, version 22, epoch 0, cached adjacency 172.17.24.1 (0x629E1B60)
0 packets, 0 bytes
  via 172.17.24.1, FastEthernet0/1, 0 dependencies
  next hop 172.17.24.1, FastEthernet0/1
  valid cached adjacency (0x629E1B60)
	Router# **show ip cef internal**
	
	IPv4 CEF is enabled and running
	VRF Default:
	 22 prefixes (22/0 fwd/non-fwd)
	 Table id 0
	 Database epoch: 0 (22 entries at this epoch)
	
	0.0.0.0/32, epoch 0, flags receive, refcount 4
	  sources: Spc
	  feature space:
	  MFI: path extension list empty
	  subblocks:
	  Special source: receive
	  ifnums: (none)
	  path 633AA3DC, path list 633A79D0, share 1, type receive
	  path_list contains no resolved destination(s). HW IPv4 notified.
	  receive
	  output chain: receive (11)
	10.10.1.1/32, epoch 0, RIB, refcount 4
	  sources: RIB
	  feature space:
	  MFI: path extension list empty
	  IPRM: 0x00038000
	  IP adj out of POS1/0 635BB2A0
	  ifnums: (none)
	  path 633A9504, path list 633A6FB8, share 1, type attached nexthop
	  path_list contains at least one resolved destination(s). HW IPv4 notified.
	  nexthop 172.17.13.1 POS1/0, adjacency IP adj out of POS1/0 635BB2A0
	  output chain: IP adj out of POS1/0 635BB2A0

show ipv6 cef internal

This feature provides the following changes to the output of the **show ipv6 cef internal** command:

- More references to pointers are added.
- The concept of output chain (chain of output features) is introduced.

The previous version of the command output is very similar to the output of the command after the Cisco Express Forwarding enhancements.

Table 7 compares the **show ipv6 cef internal** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 7 show ipv6 cef internal Command Output Before and After Cisco Express Forwarding Enhancements

Old	New
Router# **show ipv6 cef internal** IPv6 CEF is enabled and running Slow processing intvl = 1 seconds backoff level current/max 0/0 0 unresolved prefixes, 0 requiring adjacency update IPv6 CEF default table 19 prefixes tableid 0 table version 37 root 63038970 2001:1:12::/64 RIBfib Using cached adjacency 0x629E1CE0 path list pointer 62A2C310 1 path - Nexthop path_pointer 62A297B0 traffic share 1 path_list pointer 62A2C310 nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1 next_hop_len 0 adjacency pointer 629E1CE0 refcount 10 no loadinfo	Router# **show ipv6 cef internal** IPv6 CEF is enabled and running VRF Default: 20 prefixes (20/0 fwd/non-fwd) Table id 0 Database epoch: 0 (20 entries at this epoch) 2001:1:12::/64, epoch 0, RIB, refcount 3 sources: RIB feature space: MFI: path extension list empty IPRM: 0x00038000 IPV6 adj out of POS1/0 635BAFE0 ifnums: (none) path 633A9A18, path list 633A732C, share 1, type attached nexthop path_list contains at least one resolved destination(s). HW IPv6 notified. nexthop FE80::205:DCFF:FE26:4800 POS1/0, adjacency IPV6 adj out of POS1/0 635BAFE0 output chain: IPV6 adj out of POS1/0 635BAFE0

show ip cef detail

This feature provides the following changes to the output of the **show ip cef detail** command:

- IPv4 and IPv6 are now separately addressed.
- Mtrie data structure descriptions are moved to a new command, the **show ip cef tree** command (see the "New Commands for the Cisco Express Forwarding Feature" section on page 24).
- The per-prefix output is reformatted (however, the information provided is the same).
- Table 8 compares the **show ip cef detail** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 8 show ip cef detail Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

Router# **show ip cef detail**
 	
IP CEF with switching (Table Version 32), flags=0x0
  26 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
  26 leaves, 19 nodes, 23400 bytes, 53 inserts, 27 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id DF940F94
  3(0) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts: 1342 leaf, 1321 node
 	
  Table epoch: 0 (26 entries at this epoch)
 	
Adjacency Table has 3 adjacencies
  1 IPv4 adjacency
  2 IPv6 adjacencies
0.0.0.0/32, version 0, epoch 0, receive
10.10.1.1/32, version 22, epoch 0, cached adjacency 172.17.24.1
0 packets, 0 bytes
  via 172.17.24.1, FastEthernet0/1, 0 dependencies
  next hop 172.17.24.1, FastEthernet0/1
  valid cached adjacency
	Router# **show ip cef detail**
	
	IPv4 CEF is enabled and running
	VRF Default:
	 22 prefixes (22/0 fwd/non-fwd)
	 Table id 0
	 Database epoch: 0 (22 entries at this epoch)
	
	0.0.0.0/32, epoch 0, flags receive
	  Special source: receive
	  receive
	10.10.1.1/32, epoch 0
	  nexthop 172.17.13.1 POS1/0
	10.10.1.2/32, epoch 0
	  nexthop 172.17.13.1 POS1/0
	10.20.12.0/24, epoch 0
	  nexthop 172.17.13.1 POS1/0
	10.60.17.0/24, epoch 0, flags attached, connected
	  attached to FastEthernet0/0
	10.60.17.0/32, epoch 0, flags receive
	  receive
	10.60.17.251/32, epoch 0, flags receive
	  receive

show ipv6 cef detail

This feature provides the following change to the output of the **show ipv6 cef detail** command:

- Output is reformatted (the information provided is the same as before the Cisco Express Forwarding enhancements).

Table 9 compares the **show ipv6 cef detail** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 9 show ipv6 cef detail Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show ipv6 cef detail`
 	
`IPv6 CEF is enabled and running`
`Slow processing intvl = 1 seconds backoff level current/max 0/0`
`0 unresolved prefixes, 0 requiring adjacency update`
`IPv6 CEF default table`
`19 prefixes`
`2001:1:12::/64 RIBfib`
`  nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1`
`2001:2:13::/64 RIBfib`
`  nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1`
`2001:2:22::/64 RIBfib`
`  nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1`
`2001:2:24::2/128 Receive, RIBfib`
`  Receive`
`2001:2:24::/64 Attached, Connected, RIBfib`
`  attached to FastEthernet0/1`
	`Router# show ipv6 cef detail`
	
	`IPv6 CEF is enabled and running`
	`VRF Default:`
	` 20 prefixes (20/0 fwd/non-fwd)`
	` Table id 0`
	` Database epoch:  0 (20 entries at this epoch)`
	
	`2001:1:12::/64, epoch 0`
	`  nexthop FE80::205:DCFF:FE26:4800 POS1/0`
	`2001:2:13::/64, epoch 0, flags attached, connected`
	`  attached to POS1/0`
	`2001:2:13::2/128, epoch 0, flags receive`

show ip cef <prefix> internal

This feature provides the following changes to the output of the **show ip cef** *prefix* **internal** command:

- Troubleshooting is made easier with the addition of references to internal structure pointers.
- The concept of output chain (chain of output features) is introduced.

Table 10 compares the **show ip cef** *prefix* **internal** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 10 show ip cef <prefix> internal Command Output Before and After Cisco Express Forwarding Enhancements

Old	New
Router# **show ip cef 10.20.12.0/24 internal** 10.20.12.0/24, version 17, epoch 0, cached adjacency 172.17.24.1 (0x629E1B60) 0 packets, 0 bytes via 172.17.24.1, FastEthernet0/1, 0 dependencies next hop 172.17.24.1, FastEthernet0/1 valid cached adjacency (0x629E1B60)	Router# **show ip cef 172.16.1.0/24 internal** 172.16.1.0/24, epoch 0, RIB, refcount 5 sources: RIB feature space: MFI: path extension list empty IPRM: 0x00038000 IP adj out of POS1/0 635BB2A0 path 633A9504, path list 633A6FB8, share 1, type attached nexthop, for IPv4 ifnums: (none) path_list contains at least one resolved destination(s). HW IPv4 notified. nexthop 172.17.13.1 POS1/0, adjacency IP adj out of POS1/0 635BB2A0 output chain: IP adj out of POS1/0 635BB2A0

show ipv6 cef <prefix> internal

This feature provides the following changes to the output of the **show ipv6 cef** *prefix* **internal** command:

- More references to structure pointers are added.
- The concept of output chain (chain of output features) is introduced.

The previous version of the command output is very similar to the output in the command after the Cisco Express Forwarding enhancements.

Table 11 compares the **show ipv6 cef** *prefix* **internal** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 11 show ipv6 cef <prefix> internal Command Output Before and After Cisco Express Forwarding Enhancements

Old	New
Router# **show ipv6 cef 2001:2:25::/64 internal** 2001:2:25::/64 RIBfib Using cached adjacency 0x629E1CE0 path list pointer 62A2C310 1 path - Nexthop path_pointer 62A297B0 traffic share 1 path_list pointer 62A2C310 nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1 next_hop_len 0 adjacency pointer 629E1CE0 refcount 10 no loadinfo	Router# **show ipv6 cef 2001:2:25::/64 internal** 2001:2:25::/64, epoch 0, RIB, refcount 4 sources: RIB feature space: MFI: path extension list empty IPRM: 0x00038000 IPV6 adj out of POS1/0 635BAFE0 path 633A9568, path list 633A6FFC, share 1, type attached nexthop, for IPv6 ifnums: (none) path_list contains at least one resolved destination(s). HW IPv6 notified. nexthop FE80::205:DCFF:FE26:4800 POS1/0, adjacency IPV6 adj out of POS1/0 635BAFE0

show ip cef <prefix>

This feature provides the following changes to the output of the **show ip cef** *prefix* command:

- Output is reformatted; the key information provided is similar to the command output provided before the Cisco Express Forwarding enhancements.
- Adjacency information is moved to the **show adjacency** *prefix* **detail** command (see the "New Commands for the Cisco Express Forwarding Feature" section on page 24).

Table 12 compares the **show ip cef** *prefix* command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 12 show ip cef <prefix> Command Output Before and After Cisco Express Forwarding Enhancements

Old	New
Router# **show ip cef 10.20.12.0/24** 10.20.12.0/24, version 17, epoch 0, cached adjacency 172.17.24.1 0 packets, 0 bytes via 172.17.24.1, FastEthernet0/1, 0 dependencies next hop 172.17.24.1, FastEthernet0/1 valid cached adjacency	Router# **show ip cef 172.16.1.0/24** 172.16.1.0/24 nexthop 172.17.13.1 POS1/0

Note The command output of the **show ipv6** *prefix* command is the same after the Cisco Express Forwarding enhancement changes as it was before the changes.

show ip cef exact-route <source> <destination> detail

This feature provides the following change to the output of the **show ip cef exact-route** *source destination* **detail** command:

- Output is reformatted (the information provided is the same as the information provided before the Cisco Express Forwarding enhancements).

Table 13 compares the command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 13 show ip cef exact-route <source> <destination> detail Command Output Before and After Cisco Express Forwarding Enhancements

Old	New
Router# **show ip cef exact-route 172.16.1.1 172.16.1.5 detail** 172.16.1.1 -> 172.16.1.5 : FastEthernet0/1 (next hop 172.17.24.1)	Router# **show ip cef exact-route 172.16.1.3 172.16.1.2 detail** 172.16.1.3 -> 172.16.1.2 => IP adj out of FastEthernet0/1, addr 172.17.25.1

show ip cef exact-route <source> <destination>

This feature provides the following change to the output of the **show ip cef exact-route** *source destination* command:

- Output is reformatted (the information provided is the same as the information provided before the Cisco Express Forwarding enhancements).

Table 14 compares the **show ip cef exact-route** *source destination* command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 14 show ip cef exact-route <source> <destination> Command Output Before and After Cisco Express Forwarding Enhancements

Old	New
Router# **show ip cef exact-route 172.16.1.1 172.16.1.5** 172.16.1.1 -> 172.16.1.5 : FastEthernet0/1 (next hop 172.17.24.1)	Router# **show ip cef exact-route 172.16.1.3 172.16.1.2** 172.16.1.3 -> 172.16.1.2 => IP adj out of FastEthernet0/1, addr 172.17.25.1

show ip cef adjacency <interface> <next-hop>

This feature provides the following change to the output of the **show ip cef adjacency** *interface next-hop* command:

- Output is reformatted (the information provided is the same as the information provided before the Cisco Express Forwarding enhancements).

Table 15 compares the **show ip cef adjacency** *interface next-hop* command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 15 show ip cef adjacency <interface> <next-hop> Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show ip cef adjacency FastEthernet0/1 172.17.24.1`
 	
`Prefix  Next Hop  Interface`
`10.10.1.1/32  172.17.24.1`
`FastEthernet0/1`
`10.10.1.2/32  172.17.24.1`
`FastEthernet0/1`
`10.20.12.0/24  172.17.24.1`
`FastEthernet0/1`
	`Router# show ip cef adjacency FastEthernet0/1 172.17.22.1`
	
	`10.10.1.2/32`
	`  nexthop 172.17.22.1 FastEthernet0/1`
	`10.20.12.0/24`
	`  nexthop 172.17.22.1 FastEthernet0/1`

show adjacency summary

This feature provides the following change to the output of the **show adjacency summary** command:

- The new output provides a detailed description of the database, high availability information, and epoch concept information.
- The per-protocol and interface summary table is moved to the **show adjacency link** command (see the "New Commands for the Cisco Express Forwarding Feature" section on page 24).

Table 16 compares the **show adjacency summary** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 16 show adjacency summary Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show adjacency summary`
 	
`Adjacency Table has 6 adjacencies`
`  4 IPv4 adjacencies`
`  2 IPv6 adjacencies`
`  Table epoch: 0 (6 entries at this epoch)`
 	
`  Interface  IPv4 Adjacencies  IPv6 Adjacencies`
`  FastEthernet0/1  1  1`
`  FastEthernet0/0  2  0`
`  FastEthernet1/1  1  1`
	`Router# show adjacency summary`
	
	`Adjacency table has 9 adjacencies:`
	`  each adjacency consumes 348 bytes (0 bytes platform extension)`
	`  7 complete adjacencies`
	`  2 incomplete adjacencies`
	`  4 adjacencies of linktype IP`
	`  4 complete adjacencies of linktype IP`
	`  0 incomplete adjacencies of linktype IP`
	`  0 adjacencies with fixups of linktype IP`
	`  4 adjacencies with IP redirect of linktype IP`
	`  4 adjacencies of linktype IPV6`
	`  2 complete adjacencies of linktype IPV6`
	`  2 incomplete adjacencies of linktype IPV6`
	`  1 adjacency of linktype TAG`
	`  1 complete adjacency of linktype TAG`
	`  0 incomplete adjacencies of linktype TAG`
	
	`Adjacency database high availability:`
	`  Database epoch: 0 (9 entries at this epoch)`
	
	`Adjacency manager summary event processing:`
	`  Summary events epoch is 3`
	`  Summary events queue contains 0 events (high water mark 7 events)`

show adjacency detail

This feature provides the following change to the output of the **show adjacency detail** command:

- Output is reformatted (the information provided is the same as the information provided before the Cisco Express Forwarding enhancements).

Table 17 compares the **show adjacency detail** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 17 show adjacency detail Command Output Before and After Cisco Express Forwarding Enhancements

Old	New
Router# **show adjacency detail** Protocol Interface Address IP FastEthernet1/1 20.0.0.2(5) 4 packets, 456 bytes 003085641F11 00055F26F81D0800 ARP 01:47:23 Epoch: 0 IPV6 FastEthernet1/1 2011:41::2(5) 0 packets, 0 bytes 003085641F11 00055F26F81D86DD IPv6 ND never Epoch: 0	Router# **show adjacency detail** Protocol Interface Address IP FastEthernet0/1 172.17.22.1(16) 0 packets, 0 bytes epoch 0 sourced in sev-epoch 3 Encap length 14 00D001E4680000055FAF2C060800 ARP IPV6 FastEthernet0/1 2001:2:22::1(6) 0 packets, 0 bytes epoch 0 sourced in sev-epoch 3 Encap length 14 00D001E4680000055FAF2C0686DD IPv6 ND

show adjacency internal

This feature provides the following changes to the output of the **show adjacency internal** command:

- Output is reformatted.
- An output chain of features was added. Otherwise, the information provided is the same as the information provided before the Cisco Express Forwarding enhancements.

Table 18 compares the **show adjacency internal** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 18 **show adjacency internal** ***Command Output Before and After Cisco Express Forwarding Enhancements***

Old

```
Router# show adjacency internal

Protocol Interface          Address
IP       FastEthernet1/1    20.0.0.2(5)
                            4 packets, 456 bytes
                            003085641F11
                            00055F26F81D0800
                            ARP        01:32:30
                            Epoch: 0
                            Fast adjacency
enabled
                            IP redirect enabled
                            IP mtu 1500 (0x0)
                            Fixup disabled
                            Adjacency pointer
0x629E16E0, refCount 5
                            Adjacency flags
0x000000
                            Connection Id
0x000000
                            Bucket 22
IPV6     FastEthernet0/1
FE80::2D0:1FF:FEE4:6800(13)
                            0 packets, 0 bytes
                            00D001E46800
                            00055F26F80686DD
                            IPv6 ND    never
                            Epoch: 0
                            Fast adjacency
enabled
                            IPv6 redirect enabled
                            IPv6 mtu 1500 (0x0)
                            Fixup disabled
                            Adjacency pointer
0x629E1CE0, refCount 13
                            Adjacency flags
0x000000
                            Connection Id
0x000000
                            Bucket 32
```

New

```
Router# show adjacency internal

Protocol Interface          Address
IP       FastEthernet0/0    10.60.17.2(6)
                            0 packets, 0 bytes
                            epoch 0
                            sourced in sev-epoch 3
                            Encap length 14
                            00000C386D8800055FAF2C080800
                            ARP
                            Fast adjacency enabled [OK]
                            L3 mtu 1500
                            Flags (0x100E)
                            Fixup disabled
                            HWIDB/IDB pointers
0x63148358/0x63148FD8
                            IP redirect enabled
                            Switching vector: IPv4 no
fixup adj oce
                            Adjacency pointer 0x636F31A0
                            Next-hop 172.17.13.1 ...

IPV6     FastEthernet0/1    2001:2:22::1(6)
                            0 packets, 0 bytes
                            epoch 0
                            sourced in sev-epoch 3
                            Encap length 14
                            00D001E4680000055FAF2C0686DD
                            IPv6 ND
                            Fast adjacency enabled [OK]
                            L3 mtu 1500
                            Flags (0x100E)
                            Fixup disabled
                            HWIDB/IDB pointers
0x6313AD40/0x6313B9C0
                            IP redirect enabled
                            Switching vector: IPv6
adjacency oce
                            Adjacency pointer 0x531C738
                           Next-hop FE80::A8BB:FE00:6500
...
```

show cef state

This feature provides the following changes to the output of the **show cef state** command:

- New output is more concise.
- Load sharing anti-polarization ID is added to the command output.
- The **show cef state** command adds a new **capabilities** keyword. Capability details now display with the new keyword.

Table 19 compares the **show cef state** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 19 show cef state Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show cef state`
 	
`CEF Status [RP]`
`  CEF enabled/running`
`  dCEF disabled/not running`
`  CEF switching enabled/running`
`  CEF default capabilities:`
`  Always CEF switching: no`
`  Always dCEF switching: no`
`  Default CEF switching: yes`
`  Default dCEF switching: no`
`  Drop multicast packets: no`
`  OK to punt packets: yes`
`  NVGEN CEF state: no`
`  fastsend() used: yes`
`  CEF NSF capable: no`
`  RPR+/SSO standby capable: no`
`  IPC delayed func on SSO: no`
`  FIB auto repair supported: yes`
`  LCs not running at init time: no`
`  Hardware forwarding supported: no`
`  Hardware forwarding in use: no`
`  Load-sharing pr. packet supported: yes`
	`Router# show cef state`
	
	`CEF Status:`
	`  RP instance`
	`  common CEF enabled`
	`IPv4 CEF Status:`
	`  CEF enabled/running`
	`  dCEF disabled/not running`
	`  CEF switching enabled/running`
	`  universal per-destination load sharing algorithm, id A189DD49`
	`IPv6 CEF Status:`
	`  CEF enabled/running`
	`  dCEF disabled/not running`
	`  original per-destination load sharing algorithm, id A189DD49`
	
	`Router# show cef state capabilities`
	
	`CEF Capabilities:`
	`  Supported address families: IPv4 IPv6`
	`  Active address families: IPv4 IPv6`
	`  Distributed Platform: no`
	`  Warm or Hot Standby supported: no`
	`  CEF NSF capable: no`
	`  IPC delayed func on SSO: no`
	`  Hardware forwarding: no`
	`  Checker auto-repair supported: yes`
	`  Crashdump on memory failure: no`
	`  Support load-sharing alg config: yes`
	`  Blocking STANDBY_HOT until synced: no`
	`IPv4 CEF Capabilities:`
	`  Default CEF switching: yes`
	`  Always FIB switching: no`
	`  Default dCEF switching: no`
	`  Always dCEF switching: no`
	`  Drop multicast packets: no`
	`  OK to punt packets: yes`
	`  NVGEN CEF state: yes`
	`  fastsend() used: yes`
	`  Support per packet load sharing: yes`
	`  Support L4 ports in load sharing: yes`
	`  Multicast (*,G) groups in CEF: no`
	`  Install local entries from RIB: no`

Table 19 show cef state Command Output Before and After Cisco Express Forwarding Enhancements (continued)

Old	New

	`IPv6 CEF Capabilities:`[1]
	`  Default CEF switching: yes`
	`  Always FIB switching: no`
	`  Default dCEF switching: no`
	`  Always dFIB switching: no`
	`  Drop multicast packets: no`
	`  OK to punt packets: yes`
	`  NVGEN CEF state: yes`
	`  fastsend() used: yes`
	`  L4 ports in load balancing support: yes`

1. This is the continuation of the output of the **show cef state capabilities** command.

show cef timers

This feature provides the following change to the output of the **show cef timers** command:

- The command output has been updated to reflect the new timers.

Table 20 compares the **show cef timers** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 20 show cef timers Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show cef timers`
 	
`CEF background process`
`  Expiration  Type`
`|  0.740  (parent)`
`  |  0.740  ARP throttle`
`  |  0.908  adjacency update hwidb`
`  |  0.908  slow resolution`
`  |  8.572  <unknown:6240E510/0>`
 	
`CEF FIB scanner process`
`  Expiration  Type`
`|  5.764  (parent)`
`  |  5.764  checker scan-rib`
`  |  6.340  checker scan-sw-hw`
`  |  49.588  checker scan-hw-sw`
	`Router# show cef timers`
	
	`CEF background process`
	`  Expiration  Type`
	`|  13.248  (parent)`
	`  |  13.248  FIB checkers: IPv4 scan-rib-ios scanner`
	`  |  13.248  FIB checkers: IPv4 scan-ios-rib scanner`
	`  |  13.248  FIB checkers: IPv6 scan-ios-rib scanner`
	
	`Platform counter polling is not enabled`
	`IPv4 CEF background process`
	`  Expiration  Type`
	`|  0.600  (parent)`
	`  |  0.600  ARP throttle`
	`  |  0.600  adjacency update hwidb`

show ip cef epoch

This feature provides the following change to the output of the **show ip cef epoch** command:

- Adjacency epoch information is removed and is available from the **show adjacency summary** command (see the"New Commands for the Cisco Express Forwarding Feature" section on page 24).

Table 21 compares the **show ip cef epoch** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 21 show ip cef epoch Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show ip cef epoch`
 	
`CEF epoch information:`
 	
`Table: Default`
`  Table epoch: 0 (33 entries at this epoch)`
 	
`Adjacency table`
`  Table epoch: 0 (7 entries at this epoch)`
	`Router# show ip cef epoch`
	
	`Table: Default`
	`  Database epoch: 0 (24 entries at this epoch)`

show ipv6 cef epoch

This feature provides the following change to the output of the **show ipv6 cef epoch** command:

- Adjacency epoch information is removed and is available from the **show adjacency summary** command (see the "New Commands for the Cisco Express Forwarding Feature" section on page 24).

Table 22 compares the **show ipv6 cef epoch** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 22 show ipv6 cef epoch Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show ipv6 cef epoch`
 	
`CEF epoch information:`
 	
`Table: Default`
`  Table epoch: 1 (2 entries at this epoch)`
 	
`Adjacency table`
`  Table epoch: 0 (1 entries at this epoch)`
	`Router# show ipv6 cef epoch`
	
	`Table: Default`
	`  Database epoch: 1 (2 entries at this epoch)`

show ip cef unresolved detail

This feature provides the following changes to the output of the **show ip cef unresolved detail** command:

- The new command output lists only unresolved prefixes.
- IPv4 and IPv6 are now separately addressed.
- Figures related to adjacencies are moved to the **show adjacency summary** command (see the "show adjacency summary" section on page 16).

- Mtrie data structure descriptions are moved to a new command, the **show ip cef tree** command (see the "New Commands for the Cisco Express Forwarding Feature" section on page 24).
- Nothing is displayed if no unresolved adjacencies exist.

Table 23 compares the **show ip cef unresolved detail** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 23 show ip cef unresolved detail Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

Router# **show ip cef unresolved detail**
 	
IP CEF with switching (Table Version 59), flags=0x0
  34 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
  34 leaves, 22 nodes, 27640 bytes, 80 inserts, 46 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id DF940F94
  3(0) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts: 5933 leaf, 5888 node
 	
  Table epoch: 0 (34 entries at this epoch)
 	
Adjacency Table has 7 adjacencies
  4 IPv4 adjacencies
  3 IPv6 adjacencies
	Router# **show ip cef unresolved detail**
	
	IPv4 CEF is enabled and running
	VRF Default
	  25 prefixes (25/0 fwd/non-fwd)
	  Table id 0x0
	  Database epoch: 0 (25 entries at this epoch)
	
	101.1.1.1/32, epoch 0, flags rib only nolabel, rib defined all labels
	  recursive via 102.2.2.2, unresolved

show ipv6 cef unresolved detail

This feature provides the following changes to the output of the **show ipv6 cef unresolved detail** command:

- Figures related to adjacencies are moved to the **show adjacency summary** command (see the "show adjacency summary" section on page 16).
- Nothing is displayed in the output if there are no unresolved adjacencies.

Table 24 compares the **show ipv6 cef unresolved detail** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 24 show ipv6 cef unresolved detail Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show ipv6 cef unresolved detail`
 	
`IPv6 CEF is enabled and running`
`Slow processing intvl = 1 seconds backoff level current/max 0/0`
`0 unresolved prefixes, 0 requiring adjacency update`
`IPv6 CEF default table`
`20 prefixes`
	`Router# show ipv6 cef unresolved detail`
	
	`IPv6 CEF is enabled and running centrally.`
	`VRF Default`
	`  6 prefixes (6/0 fwd/non-fwd)`
	`  Table id 0x1E000000`
	`  Database epoch:  0 (6 entries at this epoch)`
	
	`2002::/128, epoch 0, flags rib only nolabel, rib defined all labels`
	`  recursive via 2003::BEEF, unresolved`

show ipv6 cef non-recursive

This feature provides the following change to the output of the **show ipv6 cef non-recursive** command:

- The path information is changed to be more consistent with IPv4 path information.

Table 25 compares the **show ipv6 cef non-recursive** command output before ("Old" heading) and after ("New" heading) the Cisco Express Forwarding enhancements.

Table 25 show ipv6 cef non-recursive Command Output Before and After Cisco Express Forwarding Enhancements

Old	New

`Router# show ipv6 cef non-recursive`
 	
`2001:1:12::/64`
`  nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1`
`2001:2:13::/64`
`  nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1`
`2001:2:22::/64`
`  nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1`
	`Router# show ipv6 cef non-recursive`
	
	`::/0`
	`  no route`
	`::/127`
	`  discard`
	`2003::/128`
	`  nexthop 3003::DEAD Ethernet2/0`
	`FE80::/10`
	`  receive for Null0`
	`FF00::/8`
	`  multicast`

New Commands for the Cisco Express Forwarding Feature

This section does not contain all new Cisco Express Forwarding commands. It contains only new commands introduced with the Cisco Express Forwarding enhancements to provide the same level of information that was available with the use of other commands before the Cisco Express Forwarding enhancements were implemented. Sample output is provided for the following new commands:

- **show adjacency link {ipv4 | ipv6}**
- **show adjacency <prefix>**
- **show adjacency <prefix> detail**
- **show {ip | ipv6} cef tree**
- **test cef table consistency detail**

show adjacency link {ipv4 | ipv6}

The **show adjacency link ipv4** command and the **show adjacency link ipv6** command display information about IPv4 and IPv6 traffic, respectively, in the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table.

Per-protocol and interface summary adjacency information was moved from the **show adjacency summary** command to the **show adjacency link** command.

Following is sample output of the **show adjacency link ipv4** command.

```
Router# show adjacency link ipv4

Protocol Interface                 Address
IP       FastEthernet0/0           10.60.17.2(6)
IP       FastEthernet0/0           10.60.17.20(6)
IP       FastEthernet0/0           10.60.17.254(7)
IP       FastEthernet0/1           172.17.22.1(16)
```

Following is sample output of the **show adjacency link ipv6** command.

```
Router# show adjacency link ipv6

Protocol Interface                 Address
IPV6     FastEthernet0/1           2001:2:22::1(6)
IPV6     FastEthernet0/1           2001:2:22::2(3) (incomplete)
IPV6     FastEthernet0/1           FE80::2D0:1FF:FEE4:6800(14)
IPV6     Serial3/0                 point2point(7)
IPV6     Serial3/1                 point2point(10
```

show adjacency <prefix>

The **show adjacency** *prefix* command shows adjacency information for the specified prefix.

Following are sample outputs from the **show adjacency** *prefix* command for an IPv4 prefix and an IPv6 prefix:

```
Router# show adjacency 172.17.22.1/24

Protocol Interface                 Address
IP       FastEthernet0/1           172.17.22.1(16)
```

```
Router# show adjacency 2001:2:22::1/64

Protocol Interface                 Address
IPV6     FastEthernet0/1           2001:2:22::1(6)
```

show adjacency <prefix> detail

The **show adjacency** *prefix* **detail** command provides additional adjacency information for a specified prefix.

Information about the adjacency epoch was removed from the **show ip cef epoch** and **show ipv6 cef epoch** commands and is available from the **show adjacency** *prefix* **detail** command.

Following are sample outputs from the **show adjacency** *prefix* **detail** command for an IPv4 prefix and an IPv6 prefix:

```
Router# show adjacency 172.17.22.1/24 detail

Protocol Interface                 Address
IP       FastEthernet0/1           172.17.22.1(16)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 3
                                   Encap length 14
                                   00D001E4680000055FAF2C060800
                                   ARP

Router# show adjacency 2001:2:22::1/64 detail

Protocol Interface                 Address
IPV6     FastEthernet0/1           2001:2:22::1(6)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 3
                                   Encap length 14
                                   00D001E4680000055FAF2C0686DD
                                   IPv6 ND
```

show {ip | ipv6} cef tree

The **show** {**ip** | **ipv6**} **cef tree** command displays summary information about the underlying data structures representing the specified FIB tree.

Mtrie data structure information was removed from several commands for the implementation of the Cisco Express Forwarding enhancements. This command provides the Mtrie information removed from the **show ip cef summary**, **show ip cef internal**, and **show ip cef detail** commands.

Following is sample output for the **show ip cef tree** command:

```
Router# show ip cef tree

VRF Default tree information:
 MTRIE/RTREE storing IPv4 addresses
 24 entries (24/0 fwd/non-fwd)
 Forwarding tree:
  Forwarding lookup routine: IPv4 mtrie 8-8-8-8 optimized
  33 inserts, 9 deletes
  8-8-8-8 stride pattern
  short mask protection enabled for <= 4 bits without process suspension
  24 leaves (672 bytes), 22 nodes (22880 bytes)
  25208 total bytes
  leaf ops: 33 inserts, 9 deletes
```

```
  leaf ops with short mask protection: 2 inserts, 1 delete
  per-prefix length stats: lookup off, insert off, delete off
  refcounts: 1356 leaf, 1324 node
  node pools:
   pool[C/8 bits]: 22 allocated (0 failed), 22880 bytes
 Non-Forwarding tree:
  38 inserts, 38 deletes
  0 leaves (0 bytes), 0 nodes (0 bytes)
  0 total bytes
```

test cef table consistency detail

The **test cef table consistency detail** command displays recorded Cisco Express Forwarding consistency records found by the following detection mechanisms: lc-detect, scan-rib-ios, scan-ios-rib, scan-lc-rp, and scan-rp-lc. The scan-lc-rp and scan-rp-lc detection mechanisms are available only on routers with line cards. You can configure the Cisco Express Forwarding prefix consistency-detection mechanisms using the **cef table consistency-check** command.

This command provides output that replaces the output provided by the removed and obsolete **show ip cef inconsistency records**, **show ip cef inconsistency now**, and **show ip cef inconsistency now detail** commands.

Following is sample output for the **test cef table consistency detail** command:

```
Router# test cef table consistency detail

full-scan-rib-ios: Checking IPv4 RIB to FIB consistency
full-scan-rib-ios: FIB checked 12 prefixes, and found 0 missing.
full-scan-ios-rib: Checking IPv4 FIB to RIB consistency
full-scan-ios-rib: Checked 12 FIB prefixes in 1 pass, and found 0 extra.
full-scan-rp-lc: Sent 26 IPv4 prefixes to linecards in 1 pass
full-scan-rp-lc: Initiated IPv4 FIB check on linecards..4..1..0..
full-scan-rp-lc: FIB IPv4 check completed on linecards..1..0..4..
full-scan-rp-lc: Linecard 4 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 1 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 0 checked 26 IPv4 prefixes (ignored 0). 0 inconsistent.
full-scan-rib-ios: Checking IPv6 RIB to FIB consistency
full-scan-rib-ios: FIB checked 16 prefixes, and found 5 missing.
full-scan-ios-rib: Checking IPv6 FIB to RIB consistency
full-scan-ios-rib: Checked 11 FIB prefixes in 1 pass, and found 0 extra.
full-scan-rp-lc: Sent 11 IPv6 prefixes to linecards in 1 pass
full-scan-rp-lc: Initiated IPv6 FIB check on linecards..4..1..0..
full-scan-rp-lc: FIB IPv6 check completed on linecards..1..4..0..
full-scan-rp-lc: Linecard 4 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 1 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
full-scan-rp-lc: Linecard 0 checked 11 IPv6 prefixes (ignored 0). 0 inconsistent.
No IPv4 inconsistencies found, check took 00:00:01.444
Warning: 5 IPv6 inconsistencies found, check took 00:00:01.240
```

Unchanged Cisco Express Forwarding show Commands

Some Cisco Express Forwarding **show** commands related to the Cisco Express Forwarding enhancements were not changed with the introduction of the enhancements. The output of the following commands was not changed:

- **show cef idb**
- **show cef interface**
- **show ip cef**
- **show ip cef non-recursive**
- **show ipv6 cef**
- **show ipv6 cef adjacency**

Additional References

The following sections provide references related to the Cisco Express Forwarding feature.

Related Documents

Related Topic	Document Title
Description of Cisco Express Forwarding commands	*Cisco IOS IP Switching Command Reference*
Description of Cisco Express Forwarding IPv6 commands	*Cisco IOS IPv6 Command Reference*
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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco Express Forwarding

Table 26 lists the release history for this feature.

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

Table 26 Feature Information for Cisco Express Forwarding

Feature Name	Releases	Feature Information
Cisco Express Forwarding Enhancements: Introduction of CLI Changes and Removal of IPv4 Fast Switching	12.4(20)T	The purpose of this document is to describe the changes based on the Cisco Express Forwarding infrastructure scalability enhancements that have been implemented to adapt to the evolution of the Internet and to support new platforms and features. The changes are the removal of IP fast switching and the introduction of command line interface (CLI) modifications. This document lists Cisco Express Forwarding CLI commands that are removed, replaced, changed, and new. To help you transition to the new CLI format, the document illustrates the output for new commands and changed commands. Enhancements to Cisco Express Forwarding enable it to operate with the Multiprotocol Label Switching (MPLS) Forwarding Infrastructure (MFI) and guarantee consistency across Cisco IOS release trains. Cisco Express Forwarding infrastructure changes were introduced and implemented in the Cisco IOS 12.2(25)S-based releases and were added for T releases in Cisco IOS Release 12.4(20)T. 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. In Cisco IOS Release 12.4(20)T, this feature was introduced.

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 (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. 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.

IDB—Interface Descriptor Block. An IDB is a special control structure internal to the Cisco IOS software that contains information such as the IP address, interface state, and packet statistics. Cisco IOS software maintains one IDB for each interface present on a platform and one IDB for each subinterface.

IPRM—IP Rewrite Manager. The IPRM is a module that manages the interaction between Cisco Express Forwarding, the IP Label Distributions Modules (LDM), and the Multiprotocol Label Switching (MPLS) Forwarding Infrastructure (MFI).

Mtrie—multiway tree. The Mtrie is a data structure in which routes are stored. The Mtrie is part of the IP lookup algorithm used in Cisco Express 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, 10.0.0.0/16 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.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

Configuring Fast Switching

First Published: February 11, 2008
Last Updated: July 11, 2008

This module describes how to configure fast switching on Cisco IOS devices and provides configuration guidelines for switching paths and tuning guidelines.

Note IP unicast fast switching is no longer supported on Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases. For these and later releases, components that do not support Cisco Express Forwarding will only work in Process Switched mode.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Configuring Fast Switching" section on page 18.

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

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

Information About Configuring Fast Switching

Before you configure fast switching you should understand the following concepts:

- Benefits of Fast Switching, page 2
- Reasons for Disabling Fast Switching, page 2
- AppleTalk Access Lists Automatically Fast Switched, page 3

Benefits of Fast Switching

Fast switching allows higher throughput by switching a packet using a cache created by the initial packet sent to a particular destination. Destination addresses are stored in the high-speed cache to expedite forwarding. Routers offer better packet-transfer performance when fast switching is enabled. Fast switching is enabled by default on all interfaces that support fast switching.

When packets are fast switched, the first packet is copied to packet memory and the destination network or host is found in the fast-switching cache. The frame is rewritten and sent to the outgoing interface that services the destination. Subsequent packets for the same destination use the same switching path. The interface processor computes the CRC.

Note IP unicast fast switching is no longer supported on Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T and later releases. For these and later releases, components that do not support Cisco Express Forwarding will only work in Process Switched mode.

Reasons for Disabling Fast Switching

Fast switching uses a cache created by previous packets to achieve a higher packet throughput. Packet transfer performance is generally better when fast switching is enabled. Fast switching also provides load sharing on a per-destination basis.

By default, fast switching is enabled on all interfaces that support fast switching. However, you may want to disable fast switching to save memory space on interface cards and to help avoid congestion when high-bandwidth interfaces are writing large amounts of information to low-bandwidth interfaces. This is especially important when using rates slower than T1.

Fast switching is not supported on serial interfaces using encapsulations other than HDLC.

Note Turning off fast switching increases system overhead because the packets are then process switched by the system's CPU.

For some diagnostics, such as debugging and packet-level tracing, you need to disable fast switching. Disabling fast switching causes the router to fall back to process switching the packets. If fast switching is running, you might only see the first packet to each destination in the output of any packet-level debugging commands. Subsequent packets to the same destination are fast switched. Many packet level debugging commands cannot process packets that are fast switched. You might want to turn off fast switching temporarily to use process switching instead while you are trying to capture information to diagnose a problem.

AppleTalk Access Lists Automatically Fast Switched

AppleTalk access lists are automatically fast switched. Access list fast switching improves the performance of AppleTalk traffic when access lists are defined on an interface.

Refer to the "Configuring AppleTalk" chapter in the *Cisco IOS AppleTalk and Novell IPX Configuration Guide* for guidelines on creating and using access lists and configuring AppleTalk.

How to Configure Fast Switching

By default, fast switching is enabled on all interfaces that support fast switching. However, you may have reasons to disable fast switching (see the "Reasons for Disabling Fast Switching" section on page 2).

The tasks in this section include enabling fast switching for some software applications, disabling fast switching for other software applications, and managing the route cache associated with fast switching on the device:

Note Fast switching is not supported for the X.25 encapsulations.

Enabling Fast Switching of IPX Directed Broadcast Packets

To enable fast switching of Internet Packet Exchange (IPX) directed broadcast packets, perform the following task. This may be useful in certain broadcast-based applications that rely on helpering.

By default, Cisco IOS software switches IPX packets that are directed to the broadcast address. Fast switching of these packets is disabled. The default behavior is to process switch directed broadcast packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipx broadcast-fastswitching**
4. **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	**ipx broadcast-fastswitching** **Example:** `Router(config)# ipx broadcast-fastswitching`	Enables the router to fast switch IPX directed broadcast packets,
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Disabling IPX Fast Switching

To disable IPX fast switching, perform the following task. IPX fast switching is enabled by default. You might want to disable fast switching for the following reasons:

- To save memory on the interface cards: fast-switching caches require more memory than those used for standard switching
- To avoid congestion on interface cards when a high-bandwidth interface is writing large amounts of information to a low-bandwidth interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipx route-cache**
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.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
Step 4	**no ipx route-cache** **Example:** `Router(config-if)# no ipx route-cache`	Disables IPX fast switching on an interface.
Step 5	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Adjusting the Route Cache for IPX

Adjusting the route cache allows you to control the size of the route cache, reduce memory consumption, and improve router performance. You accomplish these tasks by controlling the route cache size and route cache invalidation. The following sections describe these optional tasks:

- Controlling IPX Route Cache Size, page 5 (Optional)
- Controlling IPX Route Cache Entry Invalidation, page 6 (Optional)

Controlling IPX Route Cache Size

You can limit the number of entries stored in the IPX route cache to free up router memory and aid router processing.

Storing too many entries in the route cache can use a substantial amount of router memory, causing router processing to slow. This situation is most common on large networks that run network management applications for NetWare.

For example, if a network management station is responsible for managing all clients and servers in a very large (greater than 50,000 nodes) Novell network, the routers on the local segment can become inundated with route cache entries. You can set a maximum number of route cache entries on these routers to free up router memory and aid router processing.

To control IPX route cache size, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipx route-cache max-size** *size*
4. **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	**`ipx route-cache max-size`** *`size`* **Example:** `Router(config)# ipx route-cache max-size 10000`	Sets a maximum limit on the number of entries in the IPX route cache. • The *size* argument is maximum number of entries allowed in the IPX route cache. **Note** If the route cache has more entries than the specified limit, the extra entries are not deleted. However, they may be removed if route cache invalidation is in use. See the "Controlling IPX Route Cache Entry Invalidation" section on page 6" for more information on invalidating route cache entries.
Step 4	**`end`** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Controlling IPX Route Cache Entry Invalidation

You can configure the router to invalidate inactive fast-switch cache entries. If these entries remain invalidated for 1 minute, the router purges the entries from the route cache.

Purging invalidated entries reduces the size of the route cache, reduces memory consumption, and improves router performance. Purging entries also helps ensure accurate route cache information.

You specify the period of time that valid fast switch cache entries must be inactive before the router invalidates them. You can also specify the number of cache entries that the router can invalidate per minute.

To control IPX route cache entry invalidation, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipx route-cache inactivity-timeout** *period* [*rate*]
4. **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	**ipx route-cache inactivity-timeout** *period* [*rate*] **Example:** `Router(config)# ipx route-cache inactivity-timeout 5 10`	Adjusts the period and rate of route cache invalidation because of inactivity. • The *period* argument is the number of minutes that a valid cache entry may be inactive before it is invalidated. Valid values are 0 through 65,535. A value of zero disables this feature. The default is 2. • The *rate* argument is the maximum number of inactive entries that may be invalidated per minute. Valid values are 0 through 65,535. The default rate is 0 (cache entries do not age). **Note** When you use the **ipx route-cache inactivity-timeout** command with the **ipx route-cache max-size** command, you can ensure a small route cache with fresh entries.
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Enabling Padding of Odd-Length IPX Packets

Some IPX end hosts accept only even-length Ethernet packets. If the length of a packet is odd, the packet must be padded with an extra byte so that end host can receive it. By default, Cisco IOS software pads odd-length Ethernet packets.

Note However, there are cases in certain topologies where nonpadded Ethernet packets are forwarded onto a remote Ethernet network. Under specific conditions, you can enable padding on intermediate media as a temporary workaround for this problem. Note that you should perform this task only under the guidance of a customer engineer or other service representative.

To enable the padding of odd-length packets, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipx route-cache**
5. **ipx pad-process-switched-packets**
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	**interface** *type number* **Example:** `Router(config)# interface serial 0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
Step 4	**no ipx route-cache** **Example:** `Router(config-if)# no ipx route-cache`	Disables IPX fast switching

	Command or Action	Purpose
Step 5	**ipx pad-process-switched-packets** **Example:** `Router(config-if)# ipx pad-process-switched-packets`	Controls whether odd-length packets are padded so as to be sent as even-length packets on an interface.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Disabling AppleTalk Fast Switching

To disable AppleTalk fast switching on an interface, perform the following task. AppleTalk fast switching is enable by default.

See the "Reasons for Disabling Fast Switching" section on page 2 for information on when you might want to disable AppleTalk fast switching.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no appletalk route-cache**
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	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
Step 4	**no appletalk route-cache** **Example:** `Router(config-if)# no appletalk route-cache`	Disables AppleTalk fast switching.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Reenabling SMDS Fast Switching for IPX and AppleTalk Packets

Switched Multimegabit Data Service (SMDS) fast switching is enabled by default. To reenable SMDS fast switching on IPX and AppleTalk packets, if it has been disabled, perform the following task.

SMDS is a wide-area networking service offered by some Regional Bell Operating Companies (RBOCs). SMDS fast switching of IPX and AppleTalk packets provides faster packet transfer on serial links with speeds above 56 kbps. Use fast switching if you use high-speed, packet-switched, datagram-based WAN technologies such as Frame Relay offered by service providers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **encapsulation smds**
5. **ipx route-cache**
6. **appletalk route-cache**
7. **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	**interface** *type number* **Example:** `Router(config)# interface serial 0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
Step 4	**encapsulation smds** **Example:** `Router(config-if)# encapsulation smds`	Enables SMDS on the desired interface.
Step 5	**ipx route-cache** **Example:** `Router(config-if)# ipx route-cache`	Enables IPX fast switching on the interface.
Step 6	**appletalk route-cache** **Example:** `Router(config-if)# appletalk route-cache`	Enables AppleTalk fast switching on all supported interfaces.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Disabling DECnet Fast Switching

To disable fast switching of DECnet packets, perform the following task.

By default, DECnet routing software implements fast switching of DECnet packets. You might want to disable fast switching to save memory space on interface cards and to help avoid congestion when high-bandwidth interfaces are writing large amounts of information to low-bandwidth interfaces. Disabling fast switching is especially important when rates slower than T1 are used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no decnet route-cache**
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.
Step 3	**interface** *type number* **Example:** `Router(config)# interface serial 0/0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
Step 4	**no decnet route-cache** **Example:** `Router(config-if)# no decnet route-cache`	Disables fast switching of DECnet packets on a per-interface basis.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Disabling ISO CLNS Fast Switching Through the Cache

Perform the following task to disable See the "Reasons for Disabling Fast Switching" section on page 2 for information on why you might want to disable ISO CLNS fast switching through the cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **no clns route-cache**
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.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
Step 4	**no clns route-cache** **Example:** `Router(config-if)# no clns route-cache`	Disables fast switching. **Note** The cache still exists and is used after the **no clns route-cache** command is entered, but the software does not do fast switching through the cache.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Configuration Examples for Configuring Fast Switching

This section provides the following examples for configuring fast switching

- Disabling ISO CLNS Fast Switching Through the Cache: Example, page 16

Enabling Fast Switching of IPX Directed Broadcast Packets: Example

The following example shows how to enable fast switching of IPX directed broadcast packets:

```
configure terminal
ipx broadcast-fastswitching
end
```

Disabling IPX Fast Switching: Example

The following example shows how to disable IPX fast switching:

```
configure terminal
interface ethernet 0
 no ipx route-cache
 end
```

Adjusting the Route Cache for IPX: Examples

The following examples show how to adjust the route cache for IPX. This allows you to control the size of the route cache, reduce memory consumption, and improve router performance.

- Controlling IPX Route Cache Size: Example, page 14
- Controlling IPX Route Cache Entry Invalidation: Example, page 14

Controlling IPX Route Cache Size: Example

The following example show how to control the IPX route cache size:

```
configure terminal
ipx route-cache max-size 10000
end
```

In this example the cache size is set to 10000 entries. If the route cache has more entries than the specified limit, the extra entries are not deleted. However, they may be removed if route cache invalidation is in use. See the ""Controlling IPX Route Cache Entry Invalidation: Example" section on page 14"for a configuration example.

Controlling IPX Route Cache Entry Invalidation: Example

The following example shows how to control IPX route cache entry invalidations;

```
configure terminal
ipx route-cache inactivity-timeout 5 10
end
```

In this example, the inactivity period is set to 5 minutes and sets a maximum of 10 entries that can be invalidated per minute.

When you use the **ipx route-cache inactivity-timeout** command with the **ipx route-cache max-size** command, you can ensure a small route cache with fresh entries.

Enabling Padding of Odd-Length IPX Packets: Example

Note Use the **ipx pad-process-switched-packets** command only under the guidance of a customer engineer or other service representative.

The following example shows how to enable padding of odd-length IPX packets:

```
configure terminal
interface serial 0
 no ipx route-cache
 ipx pad-process-switched-packets
 end
```

In this example, the Cisco IOS software pads odd-length packets so that they are sent as even-length packets on serial interface 0.

Disabling AppleTalk Fast Switching: Example

The following example shows how to disable AppleTalk fast switching:

```
configure terminal
interface ethernet 0
 no appletalk route-cache
 end
```

Reenabling SMDS Fast Switching for IPX and AppleTalk Packets: Example

The following example shows how to reenable SMDS fast switching for IPX and AppleTalk packets if fast switching is disabled:

```
configure terminal
interface serial 0
 encapsulation smds
 ipx route-cache
 appletalk route-cache
 end
```

Disabling DECnet Fast Switching: Example

The following example show how to disable DECnet fast switching:

```
configure terminal
interface serial 0/0
 no decnet route-cache
 end
```

DECnet fast switching is disabled on a per-interface basis.

Disabling ISO CLNS Fast Switching Through the Cache: Example

The following example shows how to disable ISO CLNS fast switching through the cache:

```
configure terminal
interface ethernet 0
 no clns route-cache
 end
```

Additional References

The following sections provide references related to the Configuring Fast Switching feature.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
Overview of switching paths available on Cisco IOS devices	*Cisco IOS Switching Paths Overview*
Information on how to configure AppleTalk	*Cisco IOS AppleTalk Configuration Guide,*
Description of AppleTalk commands	*Cisco IOS AppleTalk Command Reference*
Information on how to configure Novell IPX	*Cisco IOS Novell IPX Configuration Guide*
Description of the IPX commands	*Cisco IOS Novell IPX Command Reference*
Information on how to configure SMDS packet-switched software	"Configuring SDMS" chapter in the *Access and Communication Servers Configuration Guide*
Description of SMDS commands	"SMDS Commands" chapter in the *Access and Communication Servers Command Reference*
Information on how to configure DECnet	*Cisco IOS DECnet Configuration Guide*
Description of DECnet command	*Cisco IOS DECnet Command Reference*
Information on how to configure ISO CLNS	*Cisco IOS ISO CLNS Configuration Guide*
Description of ISO CLNS commands	*Cisco IOS ISO CLNS Command Reference*

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
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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Fast Switching

Table 1 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the "Cisco IOS IP Switching Roadmap" module.

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

Table 1 Feature Information for Configuring Fast Switching

Feature Name	Releases	Feature Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS Release 12.2(1) or later. This table will be updated when feature information is added to this module.	—	—

Glossary

AppleTalk—A multilayered protocol providing internetwork routing, transaction and data stream service, naming service, and comprehensive file and print sharing.

IPX—Internetwork Packet Exchange. A NetWare protocol that routes outgoing data packets across a network. Every NetWare network has a unique address assigned when its servers are configured. IPX routers use this address to route packets through an internetwork.

ISO CLNS—International Organization for Standardization (ISO) Connectionless Network Service (CLNS). A standard for the network layer of the Open System Interconnection (OSI) model. CLNS is the OSI network layer service that does not require a circuit to be established before data is transmitted. CLNS routes messages to their destination independently of any other message.

NetWare—Popular distributed network operating system developed by Novell.

SMDS—Switched Multimegabit Data Service. A wide-area networking service offered by some Regional Bell Operating Companies (RBOCs).

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

Configuring Multicast Distributed Switching

First Published: February 11, 2008
Last Updated: May 5, 2008

This module describes the required and optional tasks for configuring Multicast Distributed Switching (MDS).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Configuring Multicast Distributed Switching" section on page 13.

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

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

Information About Multicast Distributed Switching

This section provides information that you should understand about MDS.

- Advantages of Multicast Distributed Switching, page 2
- Multicast Distributed Switching Is Disabled by Default, page 2

Advantages of Multicast Distributed Switching

Prior to MDS, IP multicast traffic was always switched at the Route Processor (RP) in the Route Switch Processor (RSP)-based platforms.

Switching multicast traffic at the RP had the following disadvantages:

- The load on the RP increased. This affected important route updates and calculations (for Border Gateway Protocol (BGP), among others) and could stall the router if the multicast load was substantial.
- The net multicast performance was limited to what a single RP could switch.

MDS solves these problems by performing distributed switching of multicast packets received at the line cards (Versatile Interface Processors [VIPs] in the case of RSP, and line cards in the case of Cisco 12000 series router). The line card is the interface card that houses the VIPs (in the case of RSP) and the line card (in the case of Cisco 12000 series router). MDS is accomplished using a forwarding data structure called a Multicast Forwarding Information Base (MFIB), which is a subset of the routing table. A copy of MFIB runs on each line card and is always kept up to date with the MFIB table of the RP.

MDS can work in conjunction with Cisco Express Forwarding or unicast distributed fast switching (DFS).

Starting with Cisco IOS Release 11.2GS, IP multicast traffic can be distributed switched on RSP-based platforms with VIPs. MDS is the only multicast switching method on the Cisco 12000 series router starting with Cisco IOS Release 11.2(11)GS.

Multicast Distributed Switching Is Disabled by Default

On the Cisco 7500 series router, the default is IP multicast fast switching. MDS is an option that is available and is disabled by default.

On the Cisco 12000 series routers, MDS is also disabled by default. To switch multicast packets on the Cisco 12000 series router, you need to configure all interfaces for MDS. MDS is the only multicast switching mode for the Cisco 12000 series router.

If MDS is not enabled on an incoming interface that is capable of MDS, incoming multicast packets are not distributed switched; the multicast packets are fast switched at the RP. Also, if the incoming interface is not capable of MDS, packets are fast switched or process-switched at the RP.

If MDS is enabled on the incoming interface, but at least one of the outgoing interfaces cannot fast switch, packets are process switched.

Note We recommended that you disable fast switching on any interface when MDS is enabled.

How to Configure Multicast Distributed Switching

This section contains the following tasks to configure MDS and to monitor and maintain MDS once it is configured:

- Configuring Multicast Distributed Switching, page 3 (required)
- Maintaining Multicast Distributed Switching, page 4 (optional)
- Monitoring Multicast Distributed Switching, page 6 (optional)

Configuring Multicast Distributed Switching

Perform the following task to configure MDS. To configure MDS, you must enable it globally and on at least one interface because MDS is an attribute of the interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing distributed**
4. **interface** *type number*
5. **ip route-cache distributed**
6. **ip mroute-cache distributed**
7. Repeat Steps 4 through 6 for each interface that you want to perform MDS.
8. **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	**`ip multicast-routing distributed`** **Example:** `Router(config)# ip multicast-routing distributed`	Enables IP multicast routing. • The **distributed** keyword enables MDS globally.

	Command or Action	Purpose
Step 4	**`interface`** *`type number`* **Example:** `Router(config)# interface ethernet 0`	Configures an interface type and enters interface configuration mode. • The *type* argument is the type of interface to be configured. • The *number* argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
Step 5	**`ip route-cache distributed`** **Example:** `Router(config-if)# ip route-cache distributed`	Enables distributed switching on the RSP. **Note** This step is required on the RSP platform only.
Step 6	**`ip mroute-cache distributed`** **Example:** `Router(config-if)# ip mroute-cache distributed`	Enables MDS on the interface. For Cisco 7500 series routers, this keyword is optional; if it is omitted, fast switching occurs. For Cisco 12000 series, this keyword is required because the Cisco 12000 series does only distributed switching.
Step 7	Repeat Steps 4 through 6 for each interface that you want to perform MDS.	—
Step 8	**`end`** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Note When you enable an interface to perform distributed switching of incoming multicast packets, you are configuring the physical interface, not the logical interface (subinterface). All subinterfaces are included in the physical interface.

Maintaining Multicast Distributed Switching

This section contains the following tasks to maintain and monitor MDS:

- Maintaining Multicast Distributed Switching on the Line Card, page 5
- Maintaining Multicast Distributed Switching on the Route Processor, page 5

Maintaining Multicast Distributed Switching on the Line Card

Perform the following task to maintain MDS on the line card.

SUMMARY STEPS

1. **enable**
2. **clear ip mds forwarding**
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`clear ip mds forwarding`** **Example:** `Router# clear ip mds forwarding`	Clears MDS information from the router, • Clears the Multicast Forwarding Information Base (MFIB) table of the line card and resynchronizes it with the RP.
Step 3	**`exit`** **Example:** `Router# exit`	Exits to user EXEC mode.

Maintaining Multicast Distributed Switching on the Route Processor

Perform the following task to maintain MDS on the RP.

SUMMARY STEPS

1. **enable**
2. **clear ip mroute** {***** | *group* [*source*]}
3. **clear ip pim interface count**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`clear ip mroute`** {**`*`** | *group* [*source*]} **Example:** `Router# clear ip mroute *`	Deletes entries from the IP multicast routing table. • The * (asterisk) keyword deletes all entries from the IP multicast routing table. • The *group* argument is either of the following: – Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the **ip host** command. – IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation. • The *source* argument is a name or address of a multicast source that is sending to the group. A source need not be a member of the group. If you specify a group name or address, you can also specify a source name or address.
Step 3	**`clear ip pim interface count`** **Example:** `Router# clear ip pim interface count`	Clears all line card counts or packet counts.
Step 4	**`exit`** **Example:** `Router# exit`	Exits to user EXEC mode.

Monitoring Multicast Distributed Switching

This section contains the following tasks to maintain and monitor MDS:

- Monitoring Multicast Distributed Switching on the Line Card, page 6
- Monitoring Multicast Distributed Switching on the Route Processor, page 8

Monitoring Multicast Distributed Switching on the Line Card

Perform the following task to monitor MDS on the line cards.

Remember that to reach a line card's console, enter the **attach** *slot#* command, using the slot number where the line card resides.

```
Router> attach 1
LC-Slot1> enable
LC-Slot1#
```

SUMMARY STEPS

1. **enable**
2. **show ip mds forwarding** [*group-address*]
3. **show ip mds summary**
4. **exit**

DETAILED STEPS

Step 1 **enable**

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

```
Router> enable
Router#
```

Step 2 **show ip mds forwarding** [*group-address*]

Use this command to display the MFIB table, forwarding information, related flags, and counts. For example:

```
Router# show ip mds forwarding

IP multicast MDFS forwarding information and statistics:

Flags: N - Not MDFS switchable, F - Not all MDFS switchable, O - OIF Null
       R - In-ratelimit, A - In-access, M - MTU mismatch, P - Register set

Interface state: Interface, Next-Hop, Mac header

(*, 224.2.170.73),

 Incoming interface: Null
  Pkts: 0, last used: never, Kbps: 0, fast-flags: N
  Outgoing interface list: Null

(192.168.62.86, 224.2.170.73) [31]
  Incoming interface: Fddi3/0/0
  Pkts: 3034, last used: 00:00:00, Kbps: 0, fast-flags: M
  Outgoing interface list:
```

Step 3 **show ip mds summary**

Use this command to display a summary of the MFIB. For example:

```
Router# show ip mds summary

IP multicast MDFS forwarding information and statistics:

Flags: N - Not MDFS switchable, F - Not all MDFS switchable, O - OIF Null
       R - In-ratelimit, A - In-access, M - MTU mismatch, P - Register set
Interface state: Interface, Next-Hop, Mac header

(*, 224.2.170.73),
  Incoming interface: Null
  Pkts: 0, last used: never, Kbps: 0, fast-flags: N

(192.168.62.86, 224.2.170.73) [31]
  Incoming interface: Fddi3/0/0
  Pkts: 3045, last used: 00:00:03, Kbps: 0, fast-flags: M
```

```
(192.168.3.7, 224.2.170.73) [334]
  Incoming interface: Fddi3/0/0
  Pkts: 0, last used: never, Kbps: 0, fast-flags: M
```

Step 4 **exit**

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

```
Router# exit
Router>
```

Monitoring Multicast Distributed Switching on the Route Processor

Perform the following task to monitor MDS on the RP.

SUMMARY STEPS

1. **enable**
2. **show ip mds stats** [**switching** | **linecard**
3. **show mds interface**
4. **show interface stats**
5. **exit**

DETAILED STEPS

Step 1 **enable**

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

```
Router> enable
Router#
```

Step 2 **show ip mds stats** [**switching** | **linecard**]

Use this command to display switching statistics or line card statistics for MDS. This example displays switching statistics:

```
Router# show ip mds stats switching

Slot Total       Switched    Drops      RPF        Punts      Failures
                                                              (switch/clone)
 1   0           0           0          0          4          0/0
 3   20260925    18014717    253        93         2247454    1/0
```

This example displays linecard statistics:

```
Router# show ip mds linecard

Slot      Status    IPC(seq/max) Q(high/route)  Reloads
 1        active    10560/10596      0/0            9
 3        active    11055/11091      0/0            9
```

Step 3 **show mds interface**

Use this command to display MDS interfaces. For example:

```
Router# show mds interface

Interface                SW-Index  HW-Index  HW IDB      FS Vector   VRF
```

```
Ethernet1/0/0            2         1         0x60C2DB40  0x602FB7A4 default
Ethernet1/0/1            3         2         0x60C32280  0x603D52B8 default
Ethernet1/0/2            4         3         0x60C35E40  0x602FB7A4 default
Ethernet1/0/3            5         4         0x60C39E60  0x603D52B8 default
Ethernet1/0/4            6         5         0x60C3D780  0x602FB7A4 default
Ethernet1/0/5            7         6         0x60C41140  0x602FB7A4 default
Ethernet1/0/6            8         7         0x60C453A0  0x602FB7A4 default
Ethernet1/0/7            9         8         0x60C48DC0  0x602FB7A4 default
POS2/0/0                 10        9         0x0                     default
POS3/0/0                 11        10        0x0                     default
Virtual-Access1          13        11        0x0                     default
Loopback0                14        12        0x0                     default
Tunnel0                  15        23        0x61C2E480  0x603D52B8  vrf1
Tunnel1                  16        24        0x61C267E0  0x603D52B8  vrf2
Ethernet1/0/3.1          17        4         0x60C39E60  0x603D52B8  vrf1
Ethernet1/0/3.2          18        4         0x60C39E60  0x603D52B8  vrf2
```

Step 4 **show interface stats**

Use this command to display numbers of packet that were process switched, fast switched, and distributed switched. For example:

```
Router# show interface stats

GigabitEthernet0/0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor          0          0        225      77625
             Route cache          0          0          0          0
  Multi-Processor Fwding        950     221250        500      57000
                   Total        950     221250        725     134625
GigabitEthernet0/1
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor          1         60        226      77685
             Route cache          0          0          0          0
  Multi-Processor Fwding        500      57000        500      57000
                   Total        501      57060        726     134685
GigabitEthernet0/2
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor          1         60        226      77685
             Route cache          0          0          0          0
  Multi-Processor Fwding          0          0          0          0
                   Total          1         60        226      77685
FastEthernet1/0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor      34015    5331012       1579     158190
             Route cache          0          0          0          0
                   Total      34015    5331012       1579     158190
```

Step 5 **exit**

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

```
Router# exit
Router>
```

Configuration Examples for Configuring Multicast Distributed Switching

This section contains examples for configuring MDS.

- Configuring Multicast Distributed Switching: Example, page 10
- Maintaining Multicast Distributed Switching: Examples, page 10

Configuring Multicast Distributed Switching: Example

The following example show how to enables MDS:

```
configure terminal
ip multicast-routing distributed
interface pos 1/0/0
 ip route-cache distributed
 ip mroute-cache distributed
 end
```

The **ip route-cache distributed** command is needed on the RSP only, not on the GSR.

Maintaining Multicast Distributed Switching: Examples

This section contains the following examples for maintaining MDS:

- Maintaining Multicast Distributed Switching on the Line Card: Example, page 10
- Maintaining Multicast Distributed Switching on the Route Processor: Example, page 10

Maintaining Multicast Distributed Switching on the Line Card: Example

The following example shows how to maintain MDS on the line card:

```
enable
clear ip mds forwarding
exit
```

In this example, the MFIB table of the line card is cleared of entries and resynchronized with the RP.

Maintaining Multicast Distributed Switching on the Route Processor: Example

The following example shows how to maintain MDS on the RP:

```
enable
clear ip mroute *
clear ip pim interface count
exit
```

In this example, all entries are deleted from the IP multicast routing table and all line card counts or packet counts are cleared.

Additional References

The following sections provide references related to the Multicast Distributed Switching feature.

Related Documents

Related Topic	Document Title
IP switching commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	*Cisco IOS IP Switching Command Reference*
Overview of switching paths available on Cisco IOS devices	*Cisco IOS Switching Paths Overview*

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
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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Multicast Distributed Switching

Table 1 lists the release history for this feature.

For information on a feature in this technology that is not documented here, see the *Cisco IOS IP Switching Features Roadmap*.

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

Table 1 Feature Information for Configuring Multicast Distributed Switching

Feature Name	Releases	Feature Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS Release 12.2(1) or later. This table will be updated when feature information is added to this module.	—	—

Glossary

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

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.

MFIB—Multicast Forwarding Information Base. A protocol-independent multicast forwarding system that contains unique multicast forwarding entries for each source or group pair known in a given network. There is a separate MFIB for every logical network (VPN) in which the router is configured. Each MFIB entry resolves a given source or group pair to an incoming interface (IIF) for reverse forwarding (RPF) checking and an outgoing interface list (olist) for multicast forwarding.

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. Processor module in the Cisco 7000 series routers that integrates the functions of the Route Processor (RP) and the Switch processor (SP).

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.