Cisco IOS IP Switching Configuration Guide

Release 12.4

Corporate 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: 408 526-4100

Customer Order Number: DOC-7817483=
Text Part Number: 78-17483-02

About Cisco IOS Software Documentation for Release 12.4 xiii

Documentation Objectives xiii

Audience xiii

Documentation Organization for Cisco IOS Release 12.4 xiv

Document Conventions xx

Obtaining Documentation xxi

Cisco.com xxi

Product Documentation DVD xxii

Ordering Documentation xxii

Documentation Feedback xxii

Cisco Product Security Overview xxiii

Reporting Security Problems in Cisco Products xxiii

Obtaining Technical Assistance xxiv

Cisco Technical Support & Documentation Website xxiv

Submitting a Service Request xxiv

Definitions of Service Request Severity xxv

Obtaining Additional Publications and Information xxv

Using Cisco IOS Software for Release 12.4 xxvii

Understanding Command Modes xxvii

Getting Help xxviii

Example: How to Find Command Options xxix

Using the no and default Forms of Commands xxxii

Saving Configuration Changes xxxii

Filtering Output from the show and more Commands xxxiii

Finding Additional Feature Support Information xxxiii

Cisco IOS Switching Paths Overview 1

Basic Router Platform Architecture and Processes 1

Cisco Routing and Switching Processes 2

Routing Processes 2

Switching Processes 3

Basic Switching Paths 4

Process Switching 4

Fast Switching 4
CEF Switching 5
dCEF Switching 5
Platform and Switching Path Correlation 6
Features That Affect Performance 6
Queueing 7
Random Early Detection (RED) 7
Compression 7
Filtering 7
Encryption 7
Accounting 7

PART 1: CISCO EXPRESS FOWARDING

Cisco Express Forwarding Features Roadmap 11

Cisco Express Forwarding Overview 13

Contents 13
Information About Cisco Express Forwarding 14
Cisco Platform Support for Central CEF and dCEF 14
CEF Benefits: Improved Performance, Scalability, and Resilience 15
Media Supported by CEF 15
Main Components of CEF Operation 16
FIB Overview 16
CEF FIB and Load Balancing 16
CEF Adjacency Tables Overview 17
Adjacency Discovery 17
Adjacency Types That Require Special Handling 17
Unresolved Adjacency 18
CEF Operation Modes: Central and Distributed CEF 18
Central CEF Mode Operation 18
Distributed CEF Mode Operation 19
CEF Features Enabled by Default 20
CEF Distributed Tunnel Switching 21
CEF-Switched Multipoint GRE Tunnels (Cisco IOS 12.2(8)T) 21
Links for the CEF Features 21
How to Configure Cisco Express Forwarding 21
Configuration Examples for Cisco Express Forwarding 22
Where to Go Next 22
Additional References 22

Related Documents 22
Standards 23
MIBs 23
RFCs 23
Technical Assistance 24
Glossary 24
Feature Information for Cisco Express Forwarding 25

Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks 27

Contents 27
Prerequisites for Configuring Cisco Express Forwarding 28
Restrictions for Configuring Cisco Express Forwarding 28
Information About Configuring Basic Cisco Express Forwarding 28
Cisco Platform Support for Central CEF and dCEF 28
CEF Benefits: Improved Performance, Scalability, and Resiliency 29
Main Components for CEF Operation 29
CEF Operation Modes: Central and Distributed CEF 30
Central CEF Mode Operation 30
Distributed CEF Mode Operation 31
How to Configure Basic Cisco Express Forwarding 32
How to Verify Basic Cisco Express Forwarding 32
Determining If the Router Is Configured for Central or Distributed CEF 32
What to Do Next 33
Verifying CEF Operation on Your Router 33
Verifying That CEF Switching Is Enabled on the Input Interface on the Router 34
Locating the Prefix in a Forwarding Table on the RP 35
Finding the CEF Output Information Associated with the Prefix on the RP 37
Verifying the Adjacency or Next-Hop Information on the RP 38
Verifying dCEF Operation on Your Router 40
Syntax for CEF Commands on Line Cards 40
Verifying That dCEF Switching Is Enabled on the Input Interface on a Line Card 40
Locating the Prefix in a Forwarding Table on a Line Card 41
Finding the dCEF Output Information Associated with the Prefix on a Line Card 43
Verifying the Adjacency or Next-Hop Information on a Line Card 44
Interpreting Information in CEF Command Output 46
Verifying That the CEF Information Looks As Expected 47
Interpreting MPLS Information in CEF Output 49
Configuration Examples for Basic Cisco Express Forwarding 51

Where to Go Next 51
Additional References 51
Related Documents 51
Standards 52
MIBs 53
RFCs 53
Technical Assistance 53
Glossary 53
Feature Information for Configuring Basic Cisco Express Forwarding 55

Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks 57
Contents 57
Prerequisites for Enabling or Disabling Central CEF or dCEF 58
Restrictions for Enabling or Disabling Central CEF or dCEF 58
Information About Enabling or Disabling Central CEF or dCEF 58
Cisco Platform Support for Central CEF and dCEF 58
When to Enable or Disable Central CEF Operation on a Router 59
When to Enable dCEF Operation on a Line Card 59
When to Enable or Disable CEF Operation on an Interface 59
How to Enable or Disable Central CEF or dCEF 60
Enabling or Disabling CEF or dCEF Operation on a Router 60
Enabling or Disabling CEF or dCEF Operation on an Interface 62
Configuration Examples for Enabling or Disabling Central CEF or dCEF 63
Enabling or Disabling CEF or dCEF Operation: Examples 64
Enabling or Disabling Central CEF or dCEF Operation on an Interface: Examples 64
Additional References 65
Related Documents 65
Standards 66
MIBs 67
RFCs 67
Technical Assistance 67
Glossary 67
Feature Information for Enabling or Disabling Central CEF or dCEF 69

Configuring a Load-Balancing Scheme for CEF Traffic 71
Contents 71
Prerequisites for Configuring a Load-Balancing Scheme for CEF Traffic 72
Restrictions for Configuring a Load-Balancing Scheme for CEF Traffic 72
Information About Configuring a Load-Balancing Scheme for CEF Traffic 72

Cisco Platform Support for Central CEF and dCEF 73
CEF Load-Balancing Overview 73
Per-Destination Load Balancing for CEF Traffic 73
Per-Packet Load Balancing for CEF Traffic 74
Load-Balancing Algorithms for CEF Traffic 74
How to Configure a Load-Balancing Scheme for CEF Traffic 74
Enabling or Disabling CEF Per-Destination Load Balancing 75
Configuring CEF Per-Packet Load Balancing 76
Selecting a CEF Load-Balancing Algorithm 77
Configuration Examples for Configuring a Load-Balancing Scheme for CEF Traffic 78
Enabling or Disabling CEF Per-Destination Load Balancing: Example 79
Configuring CEF Per-Packet Load Balancing: Example 79
Selecting a CEF Load-Balancing Algorithm: Example 79
Additional References 79
Related Documents 79
Standards 80
MIBs 80
RFCs 80
Technical Assistance 81
Glossary 81
Feature Information for Configuring a Load-Balancing Scheme for CEF Traffic 81

Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables 83

Contents 83
Prerequisites for Configuring Epochs for CEF Tables 84
Information About Configuring Epochs for CEF Tables 84
Cisco Platform Support for Central CEF and dCEF 84
Nonstop Forwarding Enhanced FIB Refresh (Cisco IOS 12.2(8)T) 85
Epoch Numbering for CEF FIB and Adjacency Tables 85
Epoch Synchronization Between the RP and Line Cards 85
Epoch Numbering for Routers That Support High Availability 86
When to Refresh the CEF or Adjacency Tables 86
How to Configure Epochs and Verify Epoch Information for CEF Tables 86
Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table 87
Beginning a New Epoch and Incrementing the Epoch Number of One or All CEF Tables 88
Verifying Epoch Information for CEF and Adjacency Tables 89
Configuration Examples for Configuring Epochs for CEF Tables 90
Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table: Example 91
Beginning a New Epoch and Incrementing the Epoch Number of One or All CEF Tables: Examples 91

Additional References 92
Related Documents 92
Standards 93
MIBs 93
RFCs 93
Technical Assistance 93
Glossary 93
Feature Information for Configuring Epochs for CEF Tables 94

Configuring CEF Consistency Checkers for Route Processors and Line Cards 97

Contents 97
Prerequisites for Configuring CEF Consistency Checkers 98
Restrictions for Configuring CEF Consistency Checkers 98
Information About Configuring CEF Consistency Checkers 98
Cisco Platform Support for Central CEF and dCEF 98
CEF Consistency Checker Types for CEF and dCEF 99
How to Configure CEF Consistency Checkers 100
Enabling CEF Consistency Checkers 100
Displaying and Clearing CEF Table Inconsistencies 101
Configuration Examples for Configuring CEF Consistency Checkers 103
Enabling CEF Consistency Checkers: Example 103
Additional References 103
Related Documents 103
Standards 104
MIBs 104
RFCs 104
Technical Assistance 105
Glossary 105
Feature Information for Configuring CEF Consistency Checkers 106

Configuring CEF Network Accounting 107

Contents 107
Prerequisites for Configuring CEF Network Accounting 108
Information About Configuring CEF Network Accounting 108
Cisco Platform Support for Central CEF and dCEF 108
Traffic Matrix Statistics That You Can Collect and View 109
TMS and CEF Nonrecursive Accounting in Backbone Routers 109
How Backbone Routers Collect TMS 110
TMS Viewing Options 113

TMS Displayed with the NDA Display Module 113
Nonrecursive Accounting Information Displayed with the show ip cef Command 114
How to Configure CEF Network Accounting 115
Configuring CEF Network Accounting 115
Enabling a Backbone Router to Collect TMS 116
Using the CLI to Enable a Backbone Router to Collect TMS 116
Enabling the NDA to Collect TMS on a Backbone Router 118
Interpreting the Statistics in the tmstats_ascii File 121
Virtual Files on the Backbone Router 121
tmstats_ascii File Header Description 121
Destination Prefix Record Description 122
Tunnel Midpoint Record Description 123
Viewing Information in the tmasinfo File: BGP Neighbor Autonomous Systems for IGP Destinations 124
Header Format for tmsasinfo File 124
Neighbor AS Record in tmsasinfo File 125
Verifying CEF Network Accounting Information 126
Configuration Examples for Configuring CEF Network Accounting 127
Configuring CEF Network Accounting: Example 127
Enabling a Backbone Router to Collect TMS Data: Example 127
IP CEF Nonrecursive Accounting Configuration: Example 128
Interpreting the Statistics in the tmstats_ascii File: Example 129
Additional References 129
Related Documents 129
Standards 130
MIBs 130
RFCs 130
Technical Assistance 130
Glossary 131
Feature Information for Configuring CEF Network Accounting 132

Customizing the Display of Recorded CEF Events 133

Contents 133
Prerequisites for Customizing the Display of Recorded CEF Events 134
Restrictions for Customizing the Display of Recorded CEF Events 134
Information About Customizing the Display of Recorded CEF Events 134
Cisco Platform Support for Central CEF and dCEF 134
CEF Event Log Overview 135
How to Customize the Display of Recorded CEF Events 135

Customizing CEF Event Logging 135
Displaying CEF Event-Log Information 136
Configuration Examples for Customizing the Display of Recorded CEF Events 138
Customizing CEF Event Logging: Example 138
Additional References 138
Related Documents 138
Standards 139
MIBs 139
RFCs 139
Technical Assistance 140
Glossary 140
Feature Information for Customizing the Display of Recorded CEF Events 141

PART 2: FAST SWITCHING

Configuring Fast Switching 145
Fast Switching Configuration Task List 145
Enabling AppleTalk Fast Switching 145
Enabling IP Fast Switching 146
Enabling Fast Switching on the Same IP Interface 146
Enabling Fast Switching of IPX Directed Broadcast Packets 147
Enabling SMDS Fast Switching 147
Disabling Fast Switching for Troubleshooting 147
Disabling AppleTalk Fast Switching 148
Disabling Banyan VINES Fast Switching 148
Disabling DECnet Fast Switching 148
Disabling IPX Fast Switching 149
Disabling ISO CLNS Fast Switching Through the Cache 149
Disabling XNS Fast Switching 149
Controlling the Route Cache 149
Controlling Route Cache Invalidation for IP 150
Displaying System and Network Statistics 150
Adjusting the Route Cache for IPX 150
Controlling IPX Route Cache Size 150
Controlling IPX Route Cache Invalidation 151
Padding Odd-Length IPX Packets 151

PART 3: MULTICAST DISTRIBUTED SWITCHING

Configuring Multicast Distributed Switching 155

MDS Configuration Task List 156

Enabling MDS 156

Monitoring and Maintaining MDS 156

MDS Configuration Example 157

About Cisco IOS Software Documentation for Release 12.4

This chapter describes the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation, technical assistance, and additional publications and information from Cisco Systems. It contains the following sections:

- Documentation Objectives, page xiii
- Audience, page xiii
- Documentation Organization for Cisco IOS Release 12.4, page xiv
- Document Conventions, page xx
- Obtaining Documentation, page xxi
- Documentation Feedback, page xxii
- Cisco Product Security Overview, page xxiii
- Obtaining Technical Assistance, page xxiv
- Obtaining Additional Publications and Information, page xxv

Documentation Objectives

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

Audience

The Cisco IOS software documentation set is intended primarily 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 software commands necessary to perform particular tasks. The Cisco IOS software 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 software release.

Documentation Organization for Cisco IOS Release 12.4

The Cisco IOS Release 12.4 documentation set consists of the configuration guide and command reference pairs listed in Table 1 and the supporting documents listed in Table 2. The configuration guides and command references are organized by technology. For the configuration guides:

- Some technology documentation, such as that for DHCP, contains features introduced in Releases 12.2T and 12.3T and, in some cases, Release 12.2S. To assist you in finding a particular feature, a roadmap document is provided.
- Other technology documentation, such as that for OSPF, consists of a chapter and accompanying Release 12.2T and 12.3T feature documents.

Note In some cases, information contained in Release 12.2T and 12.3T feature documents augments or supersedes content in the accompanying documentation. Therefore it is important to review all feature documents for a particular technology.

Table 1 lists the Cisco IOS Release 12.4 configuration guides and command references.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Description
IP	
Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 *Cisco IOS IP Addressing Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP addressing and services, including Network Address Translation (NAT), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Application Services Configuration Guide, Release 12.4 *Cisco IOS IP Application Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP application services, including IP access lists, Web Cache Communication Protocol (WCCP), Gateway Load Balancing Protocol (GLBP), Server Load Balancing (SLB), Hot Standby Router Protocol (HSRP), and Virtual Router Redundancy Protocol (VRRP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Mobility Configuration Guide, Release 12.4 *Cisco IOS IP Mobility Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Mobile IP and Cisco Mobile Networks. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Multicast Configuration Guide, Release 12.4 *Cisco IOS IP Multicast Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP multicast, including Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Source Discovery Protocol (MSDP). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4 *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP routing protocols, including Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF). The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS IP Switching Configuration Guide, Release 12.4 *Cisco IOS IP Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP switching features, including Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS). The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS IPv6 Configuration Guide, Release 12.4 *Cisco IOS IPv6 Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring IP version 6 (IPv6), including IPv6 broadband access, IPv6 data-link layer, IPv6 multicast routing, IPv6 quality of service (QoS), IPv6 routing, IPv6 services and management, and IPv6 tunnel services. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Optimized Edge Routing Configuration Guide, Release 12.4 *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Optimized Edge Routing (OER) features, including OER prefix learning, OER prefix monitoring, OER operational modes, and OER policy configuration. The command reference provides detailed information about the commands used in the configuration guide.
Security and VPN	
Cisco IOS Security Configuration Guide, Release 12.4 *Cisco IOS Security Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring various aspects of security, including terminal access security, network access security, accounting, traffic filters, router access, and network data encryption with router authentication. The command reference provides detailed information about the commands used in the configuration guide.
QoS	
Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4 *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring quality of service (QoS) features, including traffic classification and marking, traffic policing and shaping, congestion management, congestion avoidance, and signaling. The command reference provides detailed information about the commands used in the configuration guide.
LAN Switching	
Cisco IOS LAN Switching Configuration Guide, Release 12.4 *Cisco IOS LAN Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to local-area network (LAN) switching features, including configuring routing between virtual LANs (VLANs) using Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, and IEEE 802.1Q encapsulation. The command reference provides detailed information about the commands used in the configuration guide.
Multiprotocol Label Switching (MPLS)	
Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4 *Cisco IOS Multiprotocol Label Switching Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Multiprotocol Label Switching (MPLS), including MPLS Label Distribution Protocol, MPLS traffic engineering, and MPLS Virtual Private Networks (VPNs). The command reference provides detailed information about the commands used in the configuration guide.
Network Management	
Cisco IOS IP SLAs Configuration Guide, Release 12.4 *Cisco IOS IP SLAs Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the Cisco IOS IP Service Level Assurances (IP SLAs) feature. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS NetFlow Configuration Guide, Release 12.4 *Cisco IOS NetFlow Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to NetFlow features, including configuring NetFlow to analyze network traffic data, configuring NetFlow aggregation caches and export features, and configuring Simple Network Management Protocol (SNMP) and NetFlow MIB features. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Network Management Configuration Guide, Release 12.4 *Cisco IOS Network Management Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to network management features, including performing basic system management, performing troubleshooting and fault management, configuring Cisco Discovery Protocol, configuring Cisco Networking Services (CNS), configuring DistributedDirector, and configuring Simple Network Management Protocol (SNMP). The command reference provides detailed information about the commands used in the configuration guide.
Voice	
Cisco IOS Voice Configuration Library, Release 12.4 *Cisco IOS Voice Command Reference*, Release 12.4	The configuration library is a task-oriented collection of configuration guides, application guides, a troubleshooting guide, feature documents, a library preface, a voice glossary, and more. It also covers Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. In addition, the library includes documentation for IP telephony applications. The command reference provides detailed information about the commands used in the configuration library.
Wireless/Mobility	
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring a Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunication System (UMTS) network. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Mobile Wireless Home Agent Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Home Agent Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Mobile Wireless Home Agent, which is an anchor point for mobile terminals for which Mobile IP or Proxy Mobile IP services are provided. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Packet Data Serving Node (PDSN), a wireless gateway between the mobile infrastructure and standard IP networks that enables packet data services in a Code Division Multiple Access (CDMA) environment. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide, Release 12.4 *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring Cisco IOS Radio Access Network products. The command reference provides detailed information about the commands used in the configuration guide.
Long Reach Ethernet (LRE) and Digital Subscriber Line (xDSL)	
Cisco IOS Broadband and DSL Configuration Guide, Release 12.4 *Cisco IOS Broadband and DSL Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring broadband access aggregation and digital subscriber line features. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Service Selection Gateway Configuration Guide, Release 12.4 *Cisco IOS Service Selection Gateway Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Service Selection Gateway (SSG) features, including subscriber authentication, service access, and accounting. The command reference provides detailed information about the commands used in the configuration guide.
Dial—Access	
Cisco IOS Dial Technologies Configuration Guide, Release 12.4 *Cisco IOS Dial Technologies Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring lines, modems, and ISDN services. This guide also contains information about configuring dialup solutions, including solutions for remote sites dialing in to a central office, Internet service providers (ISPs), ISP customers at home offices, enterprise WAN system administrators implementing dial-on-demand routing, and other corporate environments. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS VPDN Configuration Guide, Release 12.4 *Cisco IOS VPDN Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Virtual Private Dialup Networks (VPDNs), including information about Layer 2 tunneling protocols, client-initiated VPDN tunneling, NAS-initiated VPDN tunneling, and multihop VPDN. The command reference provides detailed information about the commands used in the configuration guide.
Asynchronous Transfer Mode (ATM)	
Cisco IOS Asynchronous Transfer Mode Configuration Guide, Release 12.4 *Cisco IOS Asynchronous Transfer Mode Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring Asynchronous Transfer Mode (ATM), including WAN ATM, LAN ATM, and multiprotocol over ATM (MPOA). The command reference provides detailed information about the commands used in the configuration guide.
WAN	
Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 *Cisco IOS Wide-Area Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring wide-area network (WAN) features, including Layer 2 Tunneling Protocol Version 3 (L2TPv3); Frame Relay; Link Access Procedure, Balanced (LAPB); and X.25. The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
System Management	
Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to using Cisco IOS software to configure and maintain Cisco routers and access servers, including information about using the Cisco IOS command-line interface (CLI), loading and maintaining system images, using the Cisco IOS file system, using the Cisco IOS Web browser user interface (UI), and configuring basic file transfer services. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Interface and Hardware Component Configuration Guide, Release 12.4 *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring and managing interfaces and hardware components, including dial shelves, LAN interfaces, logical interfaces, serial interfaces, and virtual interfaces. The command reference provides detailed information about the commands used in the configuration guide.
IBM Technologies	
Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 *Cisco IOS Bridging Command Reference*, Release 12.4 *Cisco IOS IBM Networking Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring: • Bridging features, including transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and Token Ring Route Switch Module (TRRSM). • IBM network features, including data-link switching plus (DLSw+), serial tunnel (STUN), and block serial tunnel (BSTUN); Logical Link Control, type 2 (LLC2), and Synchronous Data Link Control (SDLC); IBM Network Media Translation, including SDLC Logical Link Control (SDLLC) and Qualified Logical Link Control (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. The two command references provide detailed information about the commands used in the configuration guide.
Additional and Legacy Protocols	
Cisco IOS AppleTalk Configuration Guide, Release 12.4 *Cisco IOS AppleTalk Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the AppleTalk protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS DECnet Configuration Guide, Release 12.4 *Cisco IOS DECnet Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the DECnet protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS ISO CLNS Configuration Guide, Release 12.4 *Cisco IOS ISO CLNS Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring International Organization for Standardization (ISO) Connectionless Network Service (CLNS). The command reference provides detailed information about the commands used in the configuration guide.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS Novell IPX Configuration Guide, Release 12.4 *Cisco IOS Novell IPX Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring the Novell Internetwork Packet Exchange (IPX) protocol. The command reference provides detailed information about the commands used in the configuration guide.
Cisco IOS Terminal Services Configuration Guide, Release 12.4 *Cisco IOS Terminal Services Command Reference*, Release 12.4	The configuration guide is a task-oriented guide to configuring terminal services, including DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). The command reference provides detailed information about the commands used in the configuration guide.

Table 2 lists the documents and resources that support the Cisco IOS Release 12.4 software configuration guides and command references.

Table 2 Cisco IOS Release 12.4 Supporting Documents and Resources

Document Title	Description
Cisco IOS Master Commands List, Release 12.4	An alphabetical listing of all the commands documented in the Cisco IOS Release 12.4 command references.
Cisco IOS New, Modified, Replaced, and Removed Commands, Release 12.4	A listing of all the new, modified, replaced and removed commands since Cisco IOS Release 12.3, grouped by Release 12.3T maintenance release and ordered alphabetically within each group.
Cisco IOS New and Modified Commands, Release 12.3	A listing of all the new, modified, and replaced commands since Cisco IOS Release 12.2, grouped by Release 12.2T maintenance release and ordered alphabetically within each group.
Cisco IOS System Messages, Volume 1 of 2 *Cisco IOS System Messages, Volume 2 of 2*	Listings and descriptions of Cisco IOS system messages. Not all system messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
Cisco IOS Debug Command Reference, Release 12.4	An alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, and usage guidelines.
Release Notes, Release 12.4	A description of general release information, including information about supported platforms, feature sets, platform-specific notes, and Cisco IOS software defects.
Internetworking Terms and Acronyms	Compilation and definitions of the terms and acronyms used in the internetworking industry.

Table 2 Cisco IOS Release 12.4 Supporting Documents and Resources (continued)

Document Title	Description
RFCs	RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/
MIBs	MIBs are used for network monitoring. 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

Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means 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 an SNMP community string to *public*, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords, and are used in contexts in which the italic document convention is not available, such as ASCII text.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:

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 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.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation and technical support at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Using Cisco IOS Software for Release 12.4

This chapter provides tips for understanding and configuring Cisco IOS software using the command-line interface (CLI). It contains the following sections:

- Understanding Command Modes, page xxvii
- Getting Help, page xxviii
- Using the no and default Forms of Commands, page xxxii
- Saving Configuration Changes, page xxxii
- Filtering Output from the show and more Commands, page xxxiii
- Finding Additional Feature Support Information, page xxxiii

For an overview of Cisco IOS software configuration, see the *Cisco IOS Configuration Fundamentals Configuration Guide.*

For information on the conventions used in the Cisco IOS software documentation set, see the "About Cisco IOS Software Documentation for Release 12.4" chapter.

Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to a Cisco device, the device is initially in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode by entering the **enable** command and a password (when required). From privileged EXEC mode you have access to both user EXEC and privileged EXEC commands. Most EXEC commands are used independently to observe status or to perform a specific function. For example, **show** commands are used to display important status information, and **clear** commands allow you to reset counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS 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.

Table 1 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Table 1 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.
ROM monitor	From privileged EXEC mode, use the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

For more information on command modes, see the "Using the Cisco IOS Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Provides a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.

Command	Purpose
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for "carriage return." On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 2 shows examples of how you can use the question mark (**?**) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface on a Cisco 7206 router that is running Cisco IOS Release 12.0(3).

Table 2 How to Find Command Options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to `Router#`.

`Router# configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router(config)#`.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config)# interface serial ?`
`  <0-6>  Serial interface number`
`Router(config)# interface serial 4 ?`
`  /`
`Router(config)# interface serial 4/ ?`
`  <0-3>  Serial interface number`
`Router(config)# interface serial 4/0 ?`
`<cr>`
`Router(config)# interface serial 4/0`
`Router(config-if)#`
	Enter interface configuration mode by specifying the serial interface that you want to configure using the **interface serial** global configuration command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.
	When the <cr> symbol is displayed, you can press **Enter** to complete the command.
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`.

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  load-interval  Specify interval for load calculation for an interface`
`  locaddr-priority  Assign a priority group`
`  logging  Configure logging for interface`
`  loopback  Configure internal loopback on an interface`
`  mac-address  Manually set interface MAC address`
`  mls  mls router sub/interface commands`
`  mpoa  MPOA interface configuration commands`
`  mtu  Set the interface Maximum Transmission Unit (MTU)`
`  netbios  Use a defined NETBIOS access list or enable name-caching`
`  no  Negate a command or set its defaults`
`  nrzi-encoding  Enable use of NRZI encoding`
`  ntp  Configure NTP`
`  .`
`  .`
`  .`
`Router(config-if)#`
	Enter **?** to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.

Table 2 How to Find Command Options (continued)

Command	Comment
Router(config-if)# **ip ?** Interface IP configuration subcommands: access-group Specify access control for packets accounting Enable IP accounting on this interface address Set the IP address of an interface authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp DVMRP interface commands hello-interval Configures IP-EIGRP hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures IP-EIGRP hold time . . . Router(config-if)# **ip**	Enter the command that you want to configure for the interface. This example uses the **ip** command. Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.
Router(config-if)# **ip address ?** A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# **ip address**	Enter the command that you want to configure for the interface. This example uses the **ip address** command. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword. A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.
Router(config-if)# **ip address 172.16.0.1 ?** A.B.C.D IP subnet mask Router(config-if)# **ip address 172.16.0.1**	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address. Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask. A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?`
`  secondary  Make this IP address a secondary address`
`  <cr>`
`Router(config-if)# ip address 172.16.0.1 255.255.255.0`
	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.
	Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**.
	A <cr> is displayed; you can press **Enter** to complete the command, or you can enter another keyword.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0` `Router(config-if)#`	In this example, Enter is pressed to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands can also have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Saving Configuration Changes

Use the **copy system:running-config nvram:startup-config** command or the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

command **|** {**begin | include | exclude**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
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
```

For more information on the search and filter functionality, see the "Using the Cisco IOS Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Finding Additional Feature Support Information

If you want to use a specific Cisco IOS software feature, you will need to determine in which Cisco IOS software images that feature is supported. Feature support in Cisco IOS software images depends on three main factors: the software version (called the "Release"), the hardware model (the "Platform" or "Series"), and the "Feature Set" (collection of specific features designed for a certain network environment). Although the Cisco IOS software documentation set documents feature support information for Release 12.4 as a whole, it does not generally provide specific hardware and feature set information.

To determine the correct combination of Release (software version), Platform (hardware version), and Feature Set needed to run a particular feature (or any combination of features), use Feature Navigator.

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.

Software features may also have additional limitations or restrictions. For example, a minimum amount of system memory may be required. Or there may be known issues for features on certain platforms that have not yet been resolved (called "Caveats"). For the latest information about these limitations, see the release notes for the appropriate Cisco IOS software release. Release notes provide detailed installation instructions, new feature descriptions, system requirements, limitations and restrictions, caveats, and troubleshooting information for a particular software release.

Cisco IOS Switching Paths Overview

This chapter describes switching paths that can be configured on Cisco IOS devices. It contains the following sections:

- Basic Router Platform Architecture and Processes
- Basic Switching Paths
- Features That Affect Performance

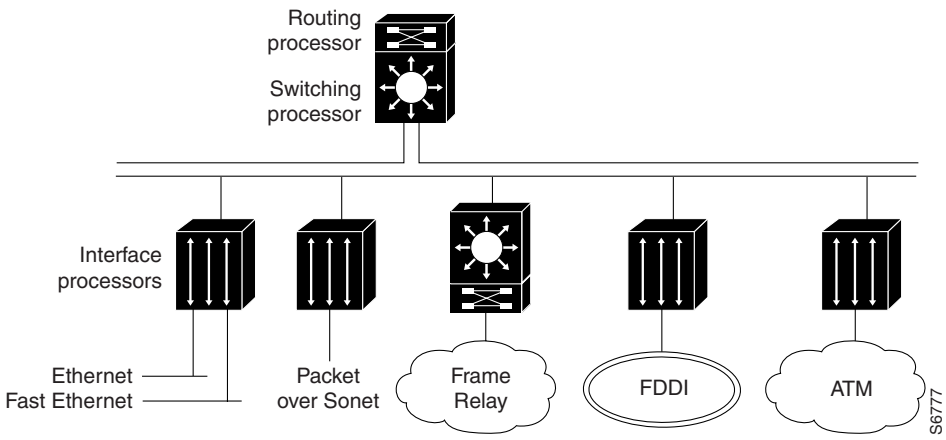
Basic Router Platform Architecture and Processes

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

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.

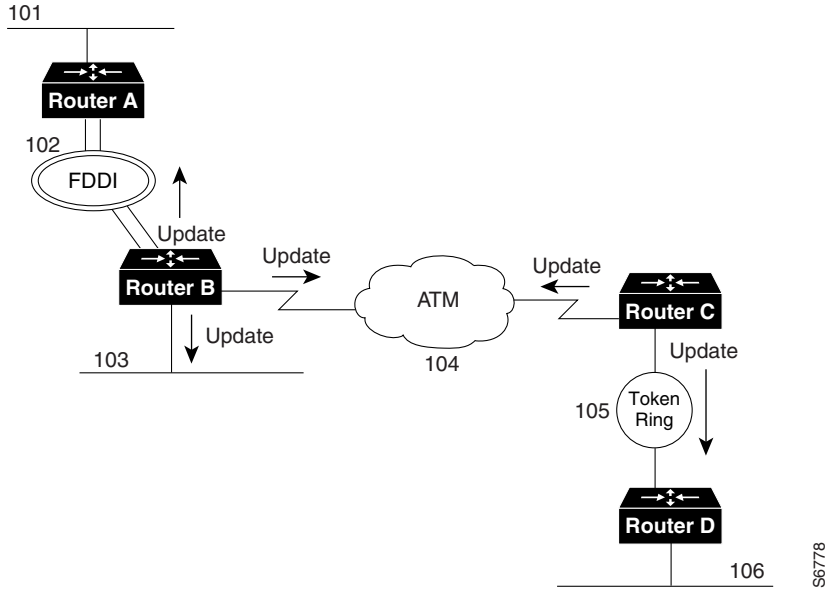
Routing Processes

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

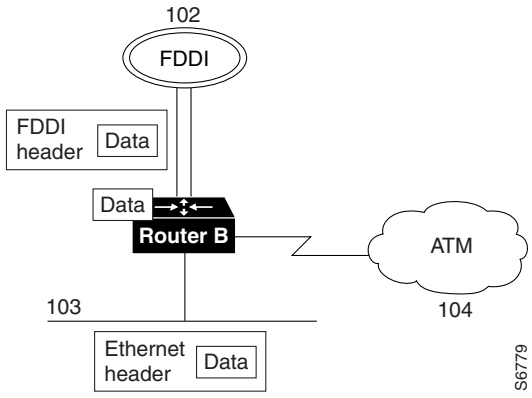


A router sends routing updates out each of its interfaces that are configured for a particular protocol. It also receives routing updates from other attached routers. From these received updates and its knowledge of attached networks, it builds a map of the network topology.

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.

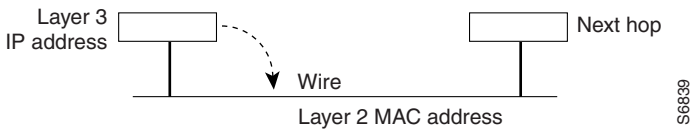
Figure 3 The Switching Process



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
- Fast Switching
- CEF Switching
- dCEF Switching

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 chapter later in this publication.

CEF Switching

When CEF mode is enabled, the CEF FIB and adjacency tables reside on the RP, and the RP performs the express forwarding. You can use CEF mode when line cards are not available for CEF switching or when you need to use features not compatible with dCEF switching. For information on configuring CEF, see the Cisco Express Forwarding Overview chapter later in this publication.

Note Beginning with Cisco IOS Release 12.0, CEF is the preferred and default switching path. NetFlow switching has been integrated into CEF switching. For information on NetFlow switching, see the Cisco Express Forwarding Overview chapter and the Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks chapter later in this publication.

dCEF Switching

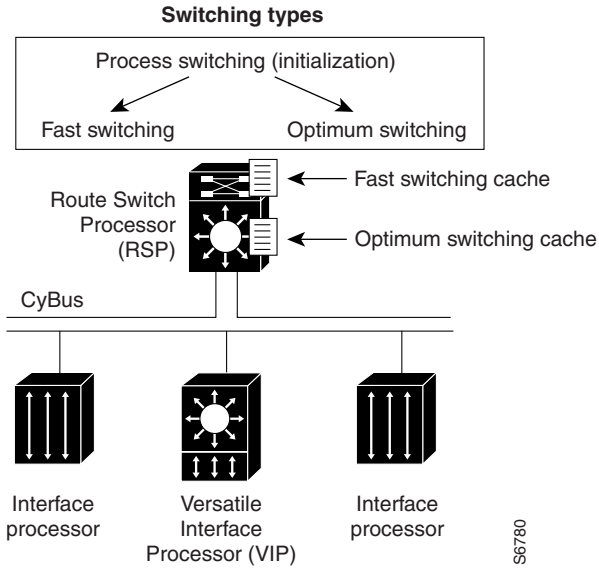
In distributed switching, the switching process occurs on VIP and other interface cards that support switching. When dCEF is enabled, line cards, such as VIP line cards or GSR line cards, maintain an identical copy of the FIB and adjacency tables. The line cards perform the express forwarding between port adapters, relieving the RSP of involvement in the switching operation. dCEF 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 dCEF, see the Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks chapter later in this publication.

For information on configuring Multicast Distributed Switching (MDS), see the Configuring Multicast Distributed Switching chapter later in this publication.

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 3 shows the correlation between Cisco IOS switching paths and routing platforms.

Table 3 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)	*protocol* **route-cache**
CEF switching	Yes	Yes	Default for IP	*protocol* **route-cache cef**
dCEF 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
- Random Early Detection (RED)
- Compression
- Filtering (using access lists)
- Encryption
- Accounting

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

Queueing

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 (RED)

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

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

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

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

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.

Cisco Systems

Part 1: Cisco Express Fowarding

Cisco Express Forwarding Features Roadmap

First Published: May 2, 2005
Last Updated: May 2, 2005

This roadmap lists the features documented in the Cisco Express Forwarding (CEF) modules and maps them to the modules in which they appear.

Feature and Release Support

Table 4 lists Cisco Express Forwarding (CEF) feature support for the following Cisco IOS software release trains:

- Cisco IOS Releases 12.2T, 12.3, and 12.3T.

Only features that were introduced or modified in Cisco IOS Release 12.2(1) or 12.0(3)S or a later release appear in the table. *Not all features may be supported in your Cisco IOS software release*.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 4 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 4 Supported Cisco Express Forwarding Features

Release	Feature Name	Feature Description	Where Documented
Cisco IOS Releases 12.2T, 12.3, and 12.3T			
12.2(8)T	CEF-Switched Multipoint GRE Tunnels	This feature enables CEF switching 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 CEF and Adjacency Tables

Cisco Express Forwarding Overview

First Published: May 2, 2005
Last Updated: May 2, 2005

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Cisco Express Forwarding" section on page 25.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Information About Cisco Express Forwarding, page 14
- How to Configure Cisco Express Forwarding, page 21
- Configuration Examples for Cisco Express Forwarding, page 22
- Where to Go Next, page 22
- Additional References, page 22
- Glossary, page 24
- Feature Information for Cisco Express Forwarding, page 25

Information About Cisco Express Forwarding

Before using CEF or distributed CEF (dCEF), you should understand the following:

- Cisco Platform Support for Central CEF and dCEF, page 14
- CEF Benefits: Improved Performance, Scalability, and Resilience, page 15
- Media Supported by CEF, page 15
- Main Components of CEF Operation, page 16
- FIB Overview, page 16
- CEF Adjacency Tables Overview, page 17
- CEF Operation Modes: Central and Distributed CEF, page 18
- CEF Features Enabled by Default, page 20
- Links for the CEF Features, page 21

Cisco Platform Support for Central CEF and dCEF

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

To find out if CEF is enabled on your platform, enter the **show ip cef** command. If CEF 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 CEF 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 CEF (dCEF) is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When dCEF is enabled on your platform, the line cards perform the express forwarding.

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

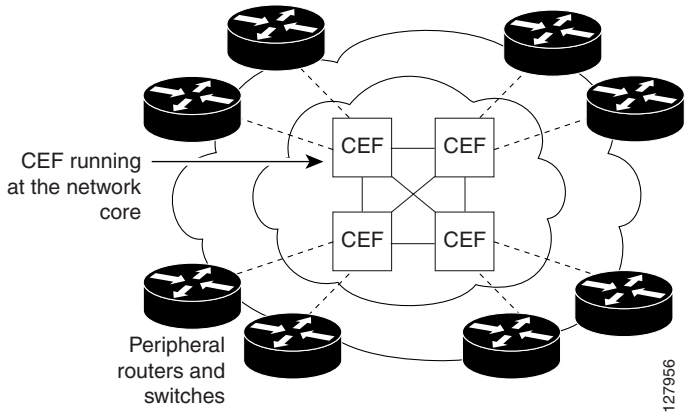
CEF Benefits: Improved Performance, Scalability, and Resilience

CEF offers the following benefits:

- Improved performance—CEF 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—CEF offers full switching capacity at each line card when dCEF mode is active. dCEF is a distributed switching mechanism that scales linearly with the number of interface cards and the bandwidth installed in the router.
- Resilience—CEF 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. CEF can switch traffic more efficiently than typical demand caching schemes.

You can use CEF in any part of a network. For example, Figure 6 shows CEF 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 6 CEF 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. CEF 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. CEF is a distributed switching mechanism that scales linearly with the number of interface cards and the bandwidth installed in the router.

Media Supported by CEF

CEF 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 CEF Operation

Information conventionally stored in a route cache is stored in several data structures for CEF switching. The data structures provide optimized lookup for efficient packet forwarding. The two main components of CEF 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 CEF 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 16.

Adjacency tables maintain Layer 2 next-hop addresses for all FIB entries. For more information, see the "CEF Adjacency Tables Overview" section on page 17.

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

- The adjacency table can be built separately from the CEF 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

CEF 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.

CEF FIB and Load Balancing

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

CEF Adjacency Tables Overview

A node is said to be adjacent to another node if the node can be reached with a single hop across a link layer (Layer 2). CEF stores forwarding information (outbound interface and MAC header rewrite) for adjacent nodes in a data structure called the adjacency table. CEF 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 17
- Adjacency Types That Require Special Handling, page 17
- Unresolved Adjacency, page 18

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 CEF 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 5.

Table 5 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, CEF 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 CEF 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.

CEF Operation Modes: Central and Distributed CEF

CEF can be enabled in one of the two modes described in the following sections:

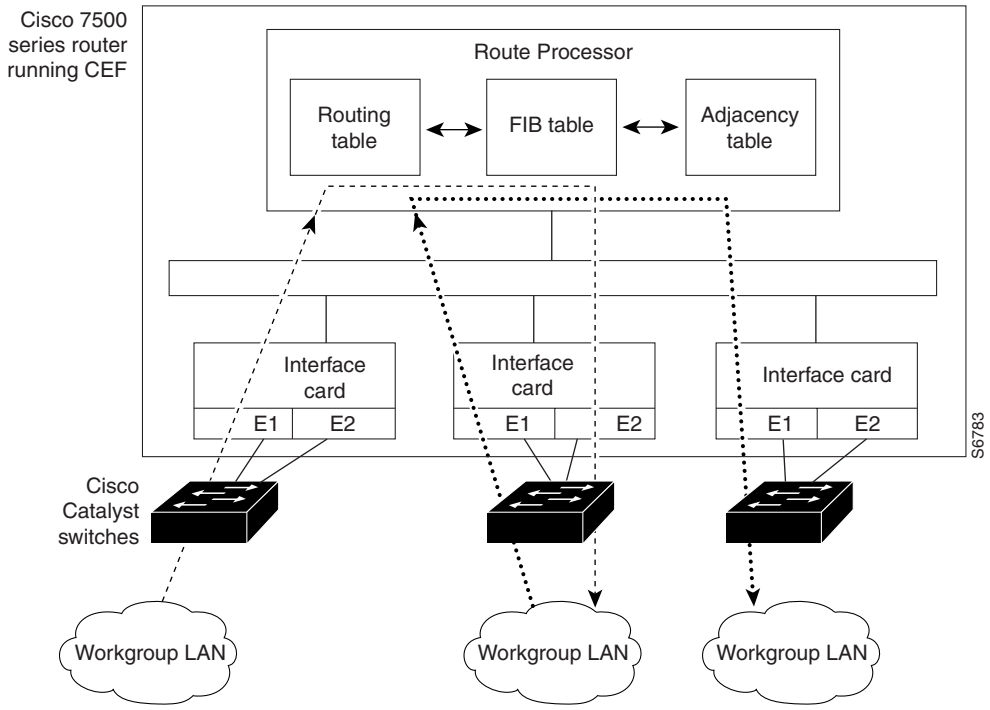
- Central CEF Mode Operation, page 18
- Distributed CEF Mode Operation, page 19

Central CEF Mode Operation

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

Figure 7 shows the relationship between the routing table, the FIB, and the adjacency table during central CEF mode operation. The Catalyst switches forward traffic from workgroup LANs to a Cisco 7500 series router on the enterprise backbone running central CEF. The RP performs the express forwarding.

Figure 7 Central CEF Mode Operation



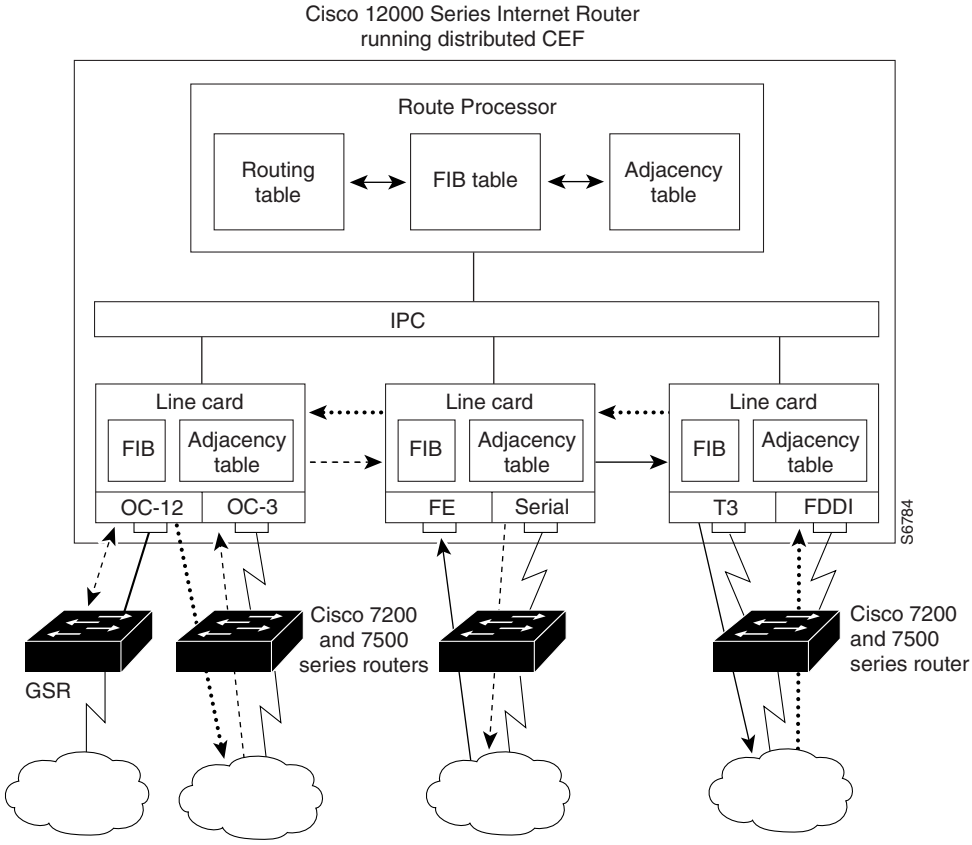
Distributed CEF Mode Operation

For additional scalability, CEF runs in the dCEF form on certain platforms by spreading processing tasks across two or more line cards. When dCEF 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.

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

Figure 8 shows the relationship between the RP and line cards when dCEF mode is active.

Figure 8 dCEF Mode Operation



In the Cisco 12000 Series Internet Router, shown in Figure 8, 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 dCEF. When a line card that does not support dCEF 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 dCEF mode.

CEF Features Enabled by Default

The following features are enabled by default when CEF is enabled:

- Per-destination load balancing and the universal load sharing algorithm (see the "Configuring a Load-Balancing Scheme for CEF Traffic" module)
- Distributed tunnel switching (see the "CEF Distributed Tunnel Switching" section on page 21)
- Multipoint generic routing encapsulation (GRE) tunnels (see the "CEF-Switched Multipoint GRE Tunnels (Cisco IOS 12.2(8)T)" section on page 21)

CEF Distributed Tunnel Switching

CEF supports distributed tunnel switching, such as that made possible by GRE tunnels. Distributed tunnel switching is enabled automatically when you enable CEF or dCEF. You do not perform any additional tasks to enable distributed tunnel switching once you enable CEF or dCEF.

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

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

Links for the CEF Features

Table 6 contains links to information about features that you can configure for use with CEF or dCEF operation.

Table 6 Features to Configure for CEF or dCEF Operation

For Information on This Feature…	See the Following Module…
Configuring and verifying basic CEF operation	"Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks"
Enabling or disabling CEF or dCEF switching/forwarding	"Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks"
Changing your load-balancing scheme	"Configuring a Load-Balancing Scheme for CEF Traffic"
Refreshing or rebuilding adjacency or CEF tables	"Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables"
Configuring CEF consistency checkers	"Configuring CEF Consistency Checkers for Route Processors and Line Cards"
Configuring network accounting for CEF	"Configuring CEF Network Accounting"
Customizing the display of recorded CEF events	"Customizing the Display of Recorded CEF 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 22 for links to configuration information for CEF 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 22 for links to configuration information for CEF features and services.

Where to Go Next

See the "Related Documents" section on page 22 for links to configuration information for CEF features and services.

Additional References

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

Related Documents

Related Topic	Document Title
List of the features documented in the Cisco Express Forwarding modules	"Cisco Express Forwarding Features Roadmap"
Tasks for verifying CEF information on your router	"Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks"
Tasks for enabling or disabling CEF or dCEF	"Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks"
Tasks for configuring a load-balancing scheme for CEF	"Configuring a Load-Balancing Scheme for CEF Traffic"
Tasks for configuring CEF consistency checkers	"Configuring CEF Consistency Checkers for Route Processors and Line Cards"
Tasks for configuring epochs for CEF tables	"Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables"
Tasks for configuring and verifying CEF network accounting	"Configuring CEF Network Accounting"
Tasks for customizing the display of recorded CEF events	"Customizing the Display of Recorded CEF Events"
Verification steps for CEF switching	*How to Verify Cisco Express Forwarding Switching*
Troubleshooting tips for incomplete adjacencies	*Troubleshooting Incomplete Adjacencies with CEF*
Description of the CEF consistency checker available for the Cisco 7500 and 12000 series routers	*Troubleshooting Prefix Inconsistencies with Cisco Express Forwarding*
Information about troubleshooting CEF routing loops and suboptimal routing	*Troubleshooting Cisco Express Forwarding Routing Loops*

Related Topic	Document Title
Causes of common CEF-related error messages on platforms running dCEF 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 tasks for the Cisco IOS software implementation of Layer 3 load balancing across multiple parallel links when CEF is used	*Troubleshooting Load Balancing Over Parallel Links Using Cisco Express Forwarding*
Troubleshooting 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*
Describes QoS features that require CEF	*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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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.

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

dCEF—distributed Cisco Express Forwarding. A mode of CEF 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 (CEF) 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 CEF 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 (CEF) tables from the Route Switch Processor (RSP) to the line card when the router is operating in distributed CEF (dCEF) 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.

Note See the Cisco *Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Cisco Express Forwarding

Table 7 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.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 7 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 7 Feature Information for Cisco Express Forwarding Overview

Feature Name	Releases	Feature Configuration Information
CEF-Switched Multipoint GRE Tunnels	12.2(8)T	This feature enables CEF switching of IP traffic to and from multipoint GRE tunnels. Prior to the introduction of this feature, only process switching was available for multipoint GRE tunnels. • "CEF-Switched Multipoint GRE Tunnels (Cisco IOS 12.2(8)T)" section on page 21

Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks

First Published: May 2, 2005
Last Updated: May 2, 2005

This module contains information about Cisco Express Forwarding (CEF) and describes the required and optional tasks for verifying CEF and distributed CEF (dCEF) operation.

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Configuring Basic Cisco Express Forwarding" section on page 55.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for Configuring Cisco Express Forwarding, page 28
- Restrictions for Configuring Cisco Express Forwarding, page 28
- Information About Configuring Basic Cisco Express Forwarding, page 28
- How to Configure Basic Cisco Express Forwarding, page 32
- How to Verify Basic Cisco Express Forwarding, page 32
- Configuration Examples for Basic Cisco Express Forwarding, page 51

- Where to Go Next, page 51
- Additional References, page 51
- Glossary, page 53
- Feature Information for Configuring Basic Cisco Express Forwarding, page 55

Prerequisites for Configuring Cisco Express Forwarding

CEF requires a software image that includes CEF and IP routing enabled on the device.

Restrictions for Configuring Cisco Express Forwarding

CEF has the following restrictions:

- The Cisco 12000 Series Internet routers operate only in dCEF mode.
- If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are process switched. Logging disables CEF.

Information About Configuring Basic Cisco Express Forwarding

Before using CEF or dCEF, you should understand the following:

- Cisco Platform Support for Central CEF and dCEF, page 28
- CEF Benefits: Improved Performance, Scalability, and Resiliency, page 29
- Main Components for CEF Operation, page 29
- CEF Operation Modes: Central and Distributed CEF, page 30
- How to Configure Basic Cisco Express Forwarding, page 32

If your network architecture requires that you disable or reenable CEF or dCEF switching/forwarding, change your load balancing scheme, refresh CEF tables, configure network accounting for CEF, or customize the display of CEF events, go to the "Related Documents" section on page 51 for links to information on these tasks. Otherwise, you need do nothing more to configure CEF or dCEF operation in your network.

Cisco Platform Support for Central CEF and dCEF

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

To find out if CEF is enabled by default on your platform, enter the **show ip cef** command. If CEF 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 CEF 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 CEF (dCEF) is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When dCEF is enabled on your platform, the line cards perform the express forwarding.

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

CEF Benefits: Improved Performance, Scalability, and Resiliency

CEF offers the following benefits:

- Improved performance—CEF 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—CEF offers full switching capacity at each line card when dCEF mode is active. dCEF is a distributed switching mechanism that scales linearly with the number of interface cards and the bandwidth installed in the router.
- Resiliency—CEF 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. CEF can switch traffic more efficiently than typical demand caching schemes.

Main Components for CEF Operation

Information conventionally stored in a route cache is stored in several data structures for CEF switching. The data structures provide optimized lookup for efficient packet forwarding. The two main components of CEF 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 CEF 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.

CEF Operation Modes: Central and Distributed CEF

CEF can be enabled in one of the two modes described in the following sections:

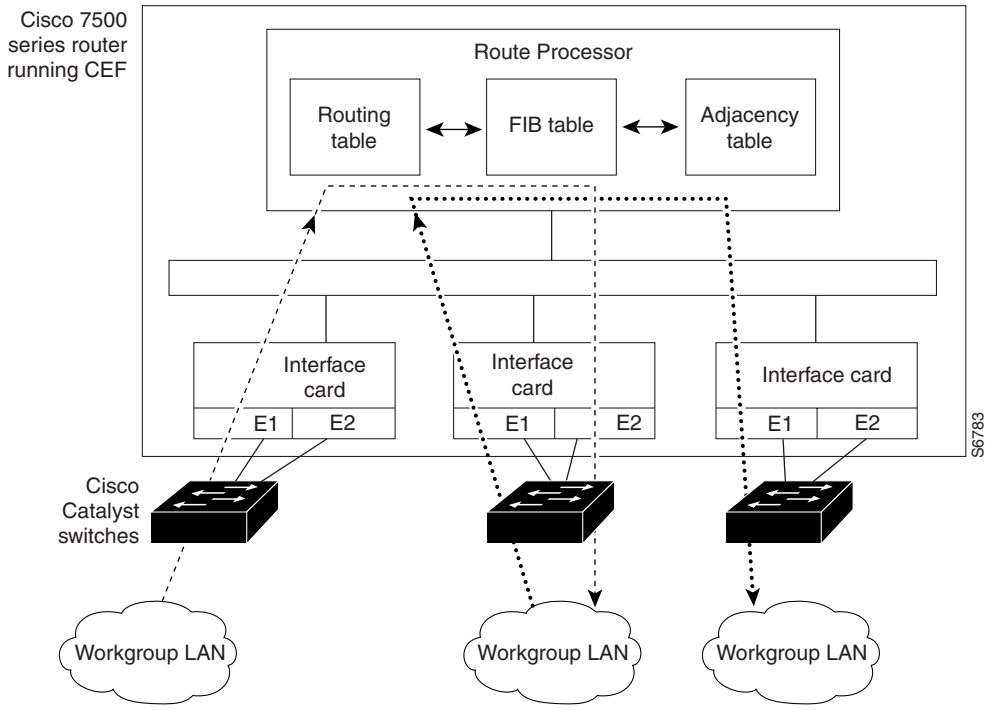
- Central CEF Mode Operation, page 30
- Distributed CEF Mode Operation, page 31

Central CEF Mode Operation

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

Figure 9 shows the relationship between the routing table, the FIB, and the adjacency table during central CEF mode operation. The Catalyst switches forward traffic from workgroup LANs to a Cisco 7500 series router on the enterprise backbone running central CEF. The RP performs the express forwarding.

Figure 9 Central CEF Mode Operation



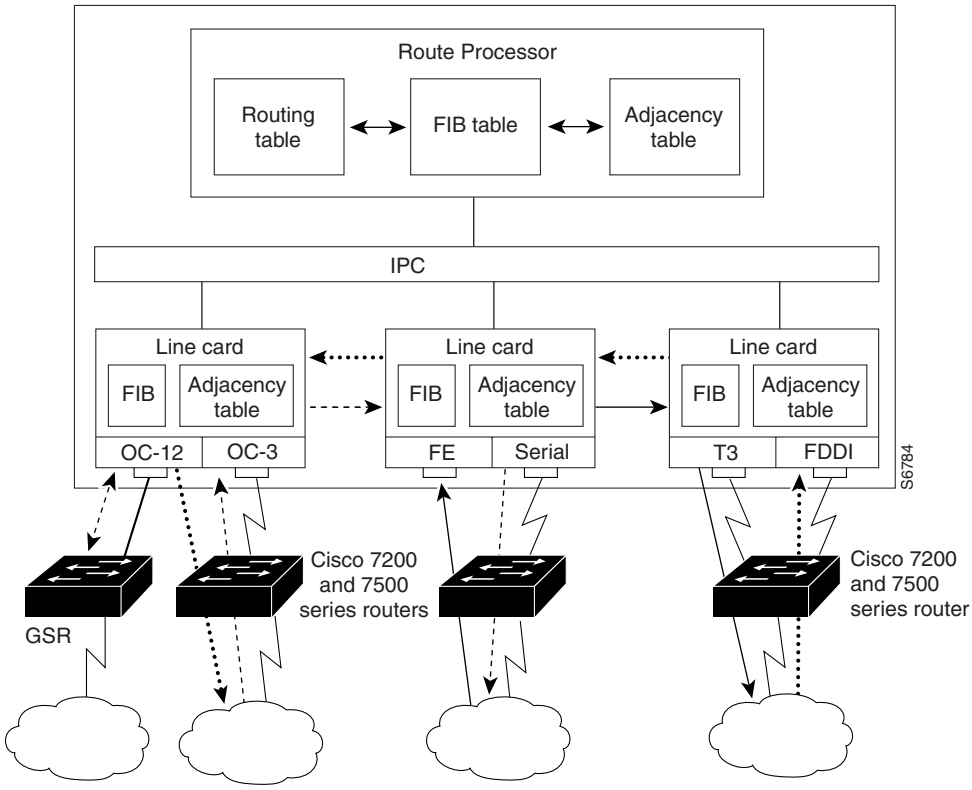
Distributed CEF Mode Operation

For additional scalability, CEF runs in the form of dCEF on certain platforms by spreading processing tasks across two or more line cards. When dCEF 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.

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

Figure 10 shows the relationship between the RP and line cards when dCEF mode is active.

Figure 10 dCEF Mode Operation



In the Cisco 12000 Series Internet Router, shown in Figure 10, 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 dCEF. When a line card that does not support dCEF 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 dCEF 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 CEF or dCEF operation.

Before you perform the remaining tasks in this section you need to know which mode of CEF is running on your router. CEF is enabled by default on the Cisco 7100, 7200, and 7500 series routers. dCEF is enabled by default on the Catalyst 6500 switch and on Cisco 12000 Series Internet routers. To determine if CEF or dCEF 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 CEF is not enabled, the entry in the command display would indicate that "IP CEF switching is disabled."

To verify basic CEF or dCEF operation, perform the following procedures and tasks:

- Determining If the Router Is Configured for Central or Distributed CEF, page 32 (required)
- Verifying CEF Operation on Your Router, page 33 (optional)
- Verifying dCEF Operation on Your Router, page 40 (optional)
- Interpreting Information in CEF Command Output, page 46 (optional)

Determining If the Router Is Configured for Central or Distributed CEF

To determine if the router is configured for CEF or dCEF, 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 CEF, complete the steps in each of the tasks on the RP in the "Verifying CEF Operation on Your Router" section on page 33.
- If the router is configured for dCEF, complete the steps in each of the tasks on the line card in the "Verifying dCEF Operation on Your Router" section on page 40. 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 CEF Operation on Your Router

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

- Verifying That CEF Switching Is Enabled on the Input Interface on the Router, page 34
- Locating the Prefix in a Forwarding Table on the RP, page 35
- Finding the CEF Output Information Associated with the Prefix on the RP, page 37
- Verifying the Adjacency or Next-Hop Information on the RP, page 38

See the "Verifying dCEF Operation on Your Router" section on page 40 for the tasks to perform for dCEF operation.

Verifying That CEF Switching Is Enabled on the Input Interface on the Router

To verify that CEF 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 CEF is enabled globally. For example:

```
Router# show ip cef

%CEF not running
```

If CEF is not running, use the **ip cef** command to enable (central) CEF or the **ip cef distributed** command to enable distributed CEF (dCEF).

When CEF or dCEF 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 CEF 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 CEF is enabled by default. The "No CEF" IP route-cache flag indicates that CEF is disabled because an administrator entered the **no ip route-cache cef** command on this interface.

To enable CEF on this interface, enter the **ip route-cache cef** command. Once you do that, the "CEF" flag indicates that CEF 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 CEF 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 CEF Output Information Associated with the Prefix on the RP

To find the CEF 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 CEF. 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 CEF 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 dCEF Operation on Your Router

Perform the following tasks, in the order presented, to verify dCEF operation on your router:

- Verifying That dCEF Switching Is Enabled on the Input Interface on a Line Card, page 40
- Locating the Prefix in a Forwarding Table on a Line Card, page 41
- Finding the dCEF Output Information Associated with the Prefix on a Line Card, page 43
- Verifying the Adjacency or Next-Hop Information on a Line Card, page 44

Syntax for CEF 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 dCEF Switching Is Enabled on the Input Interface on a Line Card

To verify that dCEF 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 CEF is enabled globally. For example:

```
Router# show ip cef

%CEF not running
```

If CEF is not running, use the **ip cef** command to enable (central) CEF or the **ip cef distributed** command to enable distributed CEF (dCEF).

When CEF or dCEF 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 dCEF 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 dCEF Output Information Associated with the Prefix on a Line Card

To find the dCEF 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.

CEF 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 CEF 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 CEF Command Output

Perform the following tasks to interpret information in CEF command output:

- Verifying That the CEF Information Looks As Expected, page 47 (optional)
- Interpreting MPLS Information in CEF Output, page 49 (optional)

Verifying That the CEF Information Looks As Expected

Perform the following tasks to verify that the CEF 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.

CEF 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 dCEF 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 dCEF 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 CEF 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 CEF Output

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

CEF and MPLS Interaction

CEF 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 CEF commands should show these processes.

The Cisco implementation of MPLS leverages the advantages of CEF. When you use a router as an MPLS edge router, CEF 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 CEF.

MPLS VPNs and CEF 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 CEF 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 CEF table, packets are forwarded to their destinations. Output from CEF commands shows details from the VRF CEF 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 CEF 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 CEF output provides MPLS information for the first adjacency. The “tag rewrite” is an equivalent of a CEF 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 CEF or dCEF operation, refer to the "Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks" module.

Additional References

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

Related Documents

Related Topic	Document Title
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 CEF or dCEF	Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks
Tasks for configuring a load-balancing scheme for CEF	Configuring a Load-Balancing Scheme for CEF Traffic

Related Topic	Document Title
Tasks for configuring CEF consistency checkers	Configuring CEF Consistency Checkers for Route Processors and Line Cards
Tasks for configuring epochs for CEF tables	Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables
Tasks for configuring and verifying CEF network accounting	Configuring CEF Network Accounting
Tasks for customizing the display of recorded CEF events	Customizing the Display of Recorded CEF Events
Verification steps for CEF switching	*How to Verify Cisco Express Forwarding Switching*
Troubleshooting tips for incomplete adjacencies	*Troubleshooting Incomplete Adjacencies with CEF*
Description and use of the CEF consistency checkers available for the Cisco 7500 and Cisco 12000 Series Internet routers	*Troubleshooting Prefix Inconsistencies with Cisco Express Forwarding*
Information about troubleshooting CEF routing loops and suboptimal routing	*Troubleshooting Cisco Express Forwarding Routing Loops*
Causes of common CEF-related error messages on platforms running dCEF 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 tasks for the Cisco IOS software implementation of Layer 3 load balancing across multiple parallel links when CEF is used	*Troubleshooting Load Balancing Over Parallel Links Using Cisco Express Forwarding*
Troubleshooting 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 CEF	*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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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.

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

dCEF—distributed Cisco Express Forwarding. A type of CEF 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 (CEF). The router uses the FIB lookup table to make destination-based switching decisions during CEF 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 (CEF) tables from the Route Switch Processor (RSP) to the line card when the router is operating in distributed CEF (dCEF) 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.

Note Refer to the Cisco *Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Configuring Basic Cisco Express Forwarding

Table 8 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.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 8 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 8 Feature Information for Configuring Basic 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.	—	—

Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks

First Published: May 2, 2005
Last Updated: May 2, 2005

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Enabling or Disabling Central CEF or dCEF" section on page 69.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for Enabling or Disabling Central CEF or dCEF, page 58
- Restrictions for Enabling or Disabling Central CEF or dCEF, page 58
- Information About Enabling or Disabling Central CEF or dCEF, page 58
- How to Enable or Disable Central CEF or dCEF, page 60
- Configuration Examples for Enabling or Disabling Central CEF or dCEF, page 63
- Additional References, page 65
- Glossary, page 67
- Feature Information for Enabling or Disabling Central CEF or dCEF, page 69

Prerequisites for Enabling or Disabling Central CEF or dCEF

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

Restrictions for Enabling or Disabling Central CEF or dCEF

Central CEF or dCEF has the following restrictions:

- The Cisco 12000 Series Internet routers operate only in dCEF mode.
- If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are process switched. Logging disables CEF.
- dCEF switching cannot be configured on the same VIP card on which distributed fast switching is configured.
- dCEF is not supported on Cisco 7200 series routers.

Restrictions for CEF or dCEF Operation on an Interface

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

Information About Enabling or Disabling Central CEF or dCEF

Before enabling or disabling CEF or dCEF, you should understand the following:

- Cisco Platform Support for Central CEF and dCEF, page 58
- When to Enable or Disable Central CEF Operation on a Router, page 59
- When to Enable dCEF Operation on a Line Card, page 59
- When to Enable or Disable CEF Operation on an Interface, page 59

For links to information about other CEF and dCEF features you can configure, refer to the following section:

- How to Enable or Disable Central CEF or dCEF, page 60

Cisco Platform Support for Central CEF and dCEF

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

To find out if CEF is enabled on your platform, enter the **show ip cef** command. If CEF 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 CEF 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 CEF (dCEF) is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When dCEF is enabled on your platform, the line cards perform the express forwarding.

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

When to Enable or Disable Central CEF Operation on a Router

Enable central CEF operation when line cards are not available for CEF switching or when you need to use features not compatible with dCEF switching. When central CEF operation is enabled, the CEF FIB and adjacency tables reside on the RP, and the RP performs express forwarding.

Disable central CEF on a router when you want to turn off central CEF 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 CEF or dCEF does not support.

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

When to Enable dCEF Operation on a Line Card

Enable dCEF 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 dCEF 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. dCEF 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 dCEF 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 CEF. When a line card that does not support CEF 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 dCEF globally, all interfaces that support dCEF are enabled by default.

When to Enable or Disable CEF Operation on an Interface

You need to decide whether or not you want CEF operation on an interface. In some instances, you might want to disable CEF or dCEF on a particular interface because that interface is configured with a feature that CEF or dCEF does not support. Because all interfaces that support CEF or dCEF are enabled by default when you enable CEF operation globally, you must use the **no** form of the **ip route-cache cef** command to turn off CEF operation on a particular interface. To reenable CEF, use the **ip route-cache cef** command. To reenable dCEF, use the **ip route-cache distributed** command.

Disabling CEF or dCEF on an interface disables CEF switching for packets forwarded to the interface, but has no effect on packets forwarded out of the interface.

When you disable CEF or dCEF, Cisco IOS software switches packets received on the interface using the next fastest switching path. For CEF, the next fastest switching path is fast switching on the RP. For dCEF, the next fastest switching path is CEF 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 CEF to be enabled on the incoming interface for packets to be CEF switched.
- Because CEF 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 CEF.
- 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 CEF or dCEF

To enable or disable CEF or dCEF, perform either of the following tasks depending on whether you want to enable or disable CEF or dCEF on the router or to enable or disable CEF or dCEF on an interface:

- Enabling or Disabling CEF or dCEF Operation on a Router, page 60 (optional)
- Enabling or Disabling CEF or dCEF Operation on an Interface, page 62 (optional)

Enabling or Disabling CEF or dCEF Operation on a Router

Perform the following task to enable or disable CEF or dCEF operation on a router. CEF 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 CEF is enabled globally and on a particular interface. If CEF 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 CEF on the route processor card.
		or
		Enables dCEF operation. CEF 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 CEF is enabled. If CEF is enabled, the output displays destination prefixes, next-hop IP addresses, and next-hop interfaces.

Enabling or Disabling CEF or dCEF Operation on an Interface

Perform the following task to enable or disable CEF or dCEF operation on an interface. CEF 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 CEF 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 CEF operation on an interface or enables CEF operation on an interface after CEF operation was disabled. or Disables dCEF operation on an interface or enables dCEF operation on an interface after dCEF 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 CEF 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 CEF or dCEF

This section contains the following configuration examples:

- Enabling or Disabling CEF or dCEF Operation: Examples, page 64
- Enabling or Disabling Central CEF or dCEF Operation on an Interface: Examples, page 64

Enabling or Disabling CEF or dCEF Operation: Examples

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

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

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

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

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

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

Enabling or Disabling Central CEF or dCEF Operation on an Interface: Examples

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

The following example shows how to disable central CEF on a particular interface:

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

The following example shows how to reenable central CEF operation on an interface:

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

The following example shows how to disable dCEF on Ethernet interface 0:

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

The following example shows how to reenable dCEF operation on Ethernet interface 0:

```
configure terminal
!
```

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

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

```
configure terminal
!

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

The following example shows how to enable dCEF operation on the router (globally) and turn off CEF 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 dCEF 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 CEF or dCEF.

Related Documents

Related Topic	Document Title
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 CEF information on your router	Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks
Tasks for configuring a load-balancing scheme for CEF	Configuring a Load-Balancing Scheme for CEF Traffic
Tasks for configuring CEF consistency checkers	Configuring CEF Consistency Checkers for Route Processors and Line Cards

Related Topic	Document Title
Tasks for configuring epochs for CEF tables	Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables
Tasks for configuring and verifying CEF network accounting	Configuring CEF Network Accounting
Tasks for customizing the display of recorded CEF events	Customizing the Display of Recorded CEF Events
Troubleshooting tips for incomplete adjacencies	*Troubleshooting Incomplete Adjacencies with CEF*
Description and use of the CEF consistency checkers available for the Cisco 7500 and 12000 series routers	*Troubleshooting Prefix Inconsistencies with Cisco Express Forwarding*
Information about troubleshooting CEF routing loops and suboptimal routing	*Troubleshooting Cisco Express Forwarding Routing Loops*
Causes of common CEF-related error messages on platforms running dCEF 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 CEF 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 CEF	*When Is CEF Required for Quality of Service*
Configuration tasks for the Dialer CEF feature	*Dialer CEF*
CEF 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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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.

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

dCEF—distributed Cisco Express Forwarding. A mode of CEF 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 (CEF) 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 CEF 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 (CEF) tables from the Route Switch Processor (RSP) to the line card when the router is operating in distributed CEF (dCEF) 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.

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.

Note Refer to the Cisco *Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Enabling or Disabling Central CEF or dCEF

Table 9 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 12.0(3)S or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 9 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 9 Feature Information for Enabling or Disabling Central CEF or dCEF

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.	—	—

Configuring a Load-Balancing Scheme for CEF Traffic

First Published: May 2, 2005
Last Updated: May 2, 2005

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

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Configuring a Load-Balancing Scheme for CEF Traffic" section on page 81.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for Configuring a Load-Balancing Scheme for CEF Traffic, page 72
- Restrictions for Configuring a Load-Balancing Scheme for CEF Traffic, page 72
- Information About Configuring a Load-Balancing Scheme for CEF Traffic, page 72
- How to Configure a Load-Balancing Scheme for CEF Traffic, page 74
- Configuration Examples for Configuring a Load-Balancing Scheme for CEF Traffic, page 78

- Additional References, page 79
- Glossary, page 81
- Feature Information for Configuring a Load-Balancing Scheme for CEF Traffic, page 81

Prerequisites for Configuring a Load-Balancing Scheme for CEF Traffic

- CEF or dCEF 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 CEF Traffic

You must globally configure load balancing on Cisco 12000 Series Internet 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 CEF Traffic

Before configuring a load-balancing scheme for CEF traffic, you should understand the following:

- Cisco Platform Support for Central CEF and dCEF, page 73
- CEF Load-Balancing Overview, page 73
- Per-Destination Load Balancing for CEF Traffic, page 73
- Per-Packet Load Balancing for CEF Traffic, page 74
- Load-Balancing Algorithms for CEF Traffic, page 74

For links to information about other CEF and dCEF features that you can configure, go to the "Additional References" section on page 79.

Cisco Platform Support for Central CEF and dCEF

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

To find out if CEF is enabled on your platform, enter the **show ip cef** command. If CEF 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 CEF 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 CEF (dCEF) is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When dCEF is enabled on your platform, the line cards perform the express forwarding.

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

CEF Load-Balancing Overview

CEF 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 CEF 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 CEF. To use per-destination load balancing, you do not perform any additional tasks once CEF 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 and Cisco 12000 Series Internet Router are configured by default to perform per-destination load balancing.

Per-Packet Load Balancing for CEF Traffic

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 CEF Traffic

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

- Original algorithm—The original CEF load-balancing algorithm produced 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.
- 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.

How to Configure a Load-Balancing Scheme for CEF Traffic

Perform the following tasks to configure and fine-tune load balancing for CEF:

- Enabling or Disabling CEF Per-Destination Load Balancing, page 75 (optional)
- Configuring CEF Per-Packet Load Balancing, page 76 (optional)
- Selecting a CEF Load-Balancing Algorithm, page 77 (optional)

Enabling or Disabling CEF Per-Destination Load Balancing

Perform this task to enable or disable CEF 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.

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.

	Command or Action	Purpose
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 CEF. • The **no ip cef load-sharing** command disables CEF 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 CEF Per-Packet Load Balancing

Perform the following task to configure CEF 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.

	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 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.
Step 4	[**no**] **ip load-sharing** [**per-packet**] [**per-destination**] **Example:** Router(config-if)# ip load-sharing per-packet	Enables load balancing for CEF. • 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 CEF Load-Balancing Algorithm

Perform the following task to select a CEF load-balancing algorithm.

The router is set to perform universal load sharing by default. 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*]}
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	**ip cef load-sharing algorithm** {**original** | **tunnel** [*id*] | **universal** [*id*]} **Example:** `Router(config)# ip cef load-sharing algorithm tunnel`	Selects a CEF 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 **universal** keyword sets the load-balancing algorithm to one that uses a source and destination and an ID hash. • The *id* argument is a fixed identifier.
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged mode.

Configuration Examples for Configuring a Load-Balancing Scheme for CEF Traffic

This section contains the following examples for configuring a load-balancing scheme for CEF traffic:

- Enabling or Disabling CEF Per-Destination Load Balancing: Example, page 79
- Configuring CEF Per-Packet Load Balancing: Example, page 79
- Selecting a CEF Load-Balancing Algorithm: Example, page 79

Enabling or Disabling CEF Per-Destination Load Balancing: Example

Per-destination load balancing is enabled by default when you enable CEF. 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 CEF Per-Packet Load Balancing: Example

The following example shows how to configure per-packet load balancing for CEF:

```
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 CEF Load-Balancing Algorithm: Example

The router is set to perform universal load balancing by default. The following example shows how to select a different CEF load-balancing algorithm:

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

Additional References

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

Related Documents

Related Topic	Document Title
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 CEF and dCEF operation	Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks

Related Topic	Document Title
Tasks for enabling or disabling CEF or dCEF	Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks
Tasks for configuring CEF consistency checkers	Configuring CEF Consistency Checkers for Route Processors and Line Cards
Tasks for configuring epochs for CEF tables	Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables
Tasks for configuring and verifying CEF network accounting	Configuring CEF Network Accounting
Tasks for customizing the display of recorded CEF events	Customizing the Display of Recorded CEF Events
Explanation of and troubleshooting information for the Cisco IOS software implementation of Layer 3 load balancing across multiple parallel links when CEF 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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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.

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

dCEF—distributed Cisco Express Forwarding. A mode of CEF 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 (CEF) 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 CEF 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 information and destination IP addresses or prefixes. The RIB is also known as the routing table.

Note Refer to the Cisco *Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Configuring a Load-Balancing Scheme for CEF Traffic

Table 10 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.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 10 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 10 Feature Information for Configuring a Load-Balancing Scheme for CEF Traffic

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.	—	—

Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables

First Published: May 2, 2005
Last Updated: Month Day, Year

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

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Configuring Epochs for CEF Tables" section on page 94.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for Configuring Epochs for CEF Tables, page 84
- Information About Configuring Epochs for CEF Tables, page 84
- How to Configure Epochs and Verify Epoch Information for CEF Tables, page 86
- Configuration Examples for Configuring Epochs for CEF Tables, page 90
- Additional References, page 92
- Glossary, page 93
- Feature Information for Configuring Epochs for CEF Tables, page 94

Prerequisites for Configuring Epochs for CEF Tables

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

Information About Configuring Epochs for CEF Tables

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

Before you configure epochs for CEF tables, you should understand the following:

- Cisco Platform Support for Central CEF and dCEF, page 84
- Nonstop Forwarding Enhanced FIB Refresh (Cisco IOS 12.2(8)T), page 85
- Epoch Numbering for CEF FIB and Adjacency Tables, page 85
- Epoch Synchronization Between the RP and Line Cards, page 85
- Epoch Numbering for Routers That Support High Availability, page 86
- When to Refresh the CEF or Adjacency Tables, page 86

(See the "Nonstop Forwarding Enhanced FIB Refresh (Cisco IOS 12.2(8)T)" section on page 85 for an explanation of the term "epoch.")

Tasks for configuring epochs for CEF 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 CEF and dCEF features you can configure, refer to the "Additional References" section on page 92.

Cisco Platform Support for Central CEF and dCEF

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

To find out if CEF is enabled on your platform, enter the **show ip cef** command. If CEF 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 CEF 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 CEF (dCEF) is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When dCEF is enabled on your platform, the line cards perform the express forwarding.

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

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 CEF database tables are being rebuilt. IP forwarding on the router is therefore uninterrupted.

NSF Enhanced FIB Refresh provides for the continuation of CEF forwarding by tracking epochs. The term "epoch" refers to a period of time. A new epoch for a CEF 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 CEF database table while the software builds a new table. This is called epoch tracking and it allows CEF forwarding to continue uninterrupted while new CEF tables are being constructed, and it makes possible a seamless switchover when the new table becomes active.

Epoch Numbering for CEF FIB and Adjacency Tables

A new epoch for a CEF 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 CEF table is created. The epoch number increases by 1 for each new revision of the CEF 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 dCEF 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 CEF table to be rebuilt, the epoch number for that table is incremented, and the table is rebuilt in place. When rebuilding is complete, "stale" entries are removed from the table. You can increment the epoch of a single table or multiple tables at the same time when you enter the **clear ip cef epoch** [**all-vrfs** | **full** | **vrf** [*table*]] command. See the "When to Refresh the CEF or Adjacency Tables" section on page 86 for information on when you might need to rebuild a CEF table.

When you display information from a CEF 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 CEF tables are incremented when an RP transitions from standby mode to active. After switchover, the active secondary RP initially has FIB and adjacency databases that are the same as those of the primary RP. When the epoch number for each table is incremented, all existing entries are considered stale. However, forwarding continues as normal. As the routing protocols start to repopulate the FIB and adjacency databases, existing and new entries receive the new epoch number, indicating that the entries have been refreshed.

When to Refresh the CEF or Adjacency Tables

You refresh or rebuild the CEF or adjacency tables when the tables contain inconsistencies.

Cisco 7500 series and Cisco 12000 Series Internet routers support dCEF, 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.

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

How to Configure Epochs and Verify Epoch Information for CEF Tables

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

- Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table, page 87 (optional)
- Beginning a New Epoch and Incrementing the Epoch Number of One or All CEF Tables, page 88 (optional)
- Verifying Epoch Information for CEF and Adjacency Tables, page 89 (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.
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 CEF Tables

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

Use the **clear ip cef epoch** command when you want to rebuild a CEF table. This command increments the epoch and flushes entries associated with the old epoch. This command also clears any inconsistencies that might exist between CEF tables on the PR and CEF tables on the line cards. If everything in the system is working correctly, the command has no effect on the CEF 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.
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 CEF 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).

	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 epochs of the adjacency table and all FIB tables.
Step 5	**exit** **Example:** `Router# exit`	Exits to user EXEC mode.

Verifying Epoch Information for CEF and Adjacency Tables

Perform the following task to verify epoch information for CEF 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 CEF information in all FIB tables, including the adjacency table, is as you expect.

In the following example, CEF 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 Epochs for CEF Tables

This section contains the following epoch configuration examples:

- Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table: Example, page 91
- Beginning a New Epoch and Incrementing the Epoch Number of One or All CEF Tables: Examples, page 91

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 CEF Tables: Examples

The following example shows how to begin a new epoch and increment the epoch number of all CEF 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 CEF tables.

Related Documents

Related Topic	Document Title
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 CEF and dCEF operation	Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks
Tasks for enabling or disabling CEF or dCEF	Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks
Tasks for configuring a load-balancing scheme for CEF	Configuring a Load-Balancing Scheme for CEF Traffic
Tasks for configuring CEF consistency checkers	Configuring CEF Consistency Checkers for Route Processors and Line Cards
Tasks for configuring and verifying CEF network accounting	Configuring CEF Network Accounting
Tasks for customizing the display of recorded CEF events	Customizing the Display of Recorded CEF Events
Troubleshooting tips for incomplete adjacencies	*Troubleshooting Incomplete Adjacencies with CEF*
Description of the CEF consistency checker 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 CEF is used	*Troubleshooting Load Balancing Over Parallel Links Using Cisco Express Forwarding*
Causes of common CEF-related error messages on platforms running dCEF switching (Cisco 7500 series routers and Cisco 12000 Series Internet routers) and how to troubleshoot them	*Troubleshooting Cisco Express Forwarding-Related Error Messages*
Troubleshooting 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*

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

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.

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

dCEF—distributed Cisco Express Forwarding. A mode of CEF 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 (CEF) 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 CEF 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.

Note Refer to the Cisco *Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Configuring Epochs for CEF Tables

Table 11 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.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 11 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 11 Feature Information for Configuring Epochs for CEF 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 85 • Epoch Numbering for CEF FIB and Adjacency Tables, page 85 • Epoch Synchronization Between the RP and Line Cards, page 85 • Epoch Numbering for Routers That Support High Availability, page 86 • When to Refresh the CEF or Adjacency Tables, page 86 • Beginning a New Epoch and Incrementing the Epoch Number of the Adjacency Table, page 87 • Beginning a New Epoch and Incrementing the Epoch Number of One or All CEF Tables, page 88 • Verifying Epoch Information for CEF and Adjacency Tables, page 89

Configuring CEF Consistency Checkers for Route Processors and Line Cards

First Published: May 2, 2005
Last Updated: May 2, 2005

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

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Configuring CEF Consistency Checkers" section on page 106.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for Configuring CEF Consistency Checkers, page 98
- Restrictions for Configuring CEF Consistency Checkers, page 98
- Information About Configuring CEF Consistency Checkers, page 98
- How to Configure CEF Consistency Checkers, page 100
- Configuration Examples for Configuring CEF Consistency Checkers, page 103
- Additional References, page 103

- Glossary, page 105
- Feature Information for Configuring CEF Consistency Checkers, page 106

Prerequisites for Configuring CEF Consistency Checkers

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

Restrictions for Configuring CEF Consistency Checkers

The CEF consistency checkers lc-detect and scan-lc apply only to devices that have dCEF enabled.

Information About Configuring CEF Consistency Checkers

Before configuring CEF consistency checkers, you should understand the following:

- Cisco Platform Support for Central CEF and dCEF, page 98
- CEF Consistency Checker Types for CEF and dCEF, page 99

For links to information about other CEF and dCEF features that you can configure, refer to the following section:

- How to Configure CEF Consistency Checkers, page 100

Cisco Platform Support for Central CEF and dCEF

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

To find out if CEF is enabled on your platform, enter the **show ip cef** command. If CEF 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 CEF 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 CEF (dCEF) is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When dCEF is enabled on your platform, the line cards perform the express forwarding.

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

CEF Consistency Checker Types for CEF and dCEF

CEF 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

CEF supports passive and active consistency checkers that run independently to uncover these forwarding inconsistencies. Table 12 describes the consistency checkers and indicates whether the checker operates on the RP or the line card.

Table 12 Types of CEF Consistency Checkers

Checker Type	Operates On	Description
Lc-detect	Line card	(dCEF 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	(dCEF 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.

CEF 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 CEF system error messages and by issuing CEF **debug** and **show** commands.

For CEF consistency checker system error messages, refer to the *12.3 T System Message Guide*.

How to Configure CEF Consistency Checkers

Perform the following tasks to configure CEF consistency checkers:

- Enabling CEF Consistency Checkers, page 100 (optional)
- Displaying and Clearing CEF Table Inconsistencies, page 101 (optional)

Enabling CEF Consistency Checkers

Perform the following task to enable CEF 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.

	Command or Action	Purpose
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 CEF 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.
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 CEF Table Inconsistencies

Perform the following task to display and clear CEF 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 CEF 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 CEF 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 CEF inconsistency statistics and records found by the CEF consistency checkers. For example:

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

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

Use this command to clear CEF information from line cards. For example:

```
Router# clear cef linecard
```

Step 5 **show ip cef inconsistency**

Use this command to verify that CEF 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 CEF Consistency Checkers

This section contains the following CEF consistency checker configuration example: Enabling CEF Consistency Checkers: Example, page 103

Enabling CEF Consistency Checkers: Example

The following example shows how to enable the scan-rp CEF 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 CEF consistency checkers.

Related Documents

Related Topic	Document Title
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

Related Topic	Document Title
Tasks for verifying basic CEF and dCEF operation	Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks
Tasks for enabling or disabling CEF or dCEF	Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks
Tasks for configuring a load-balancing scheme for CEF	Configuring a Load-Balancing Scheme for CEF Traffic
Tasks for configuring epochs for CEF tables	Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables
Tasks for configuring and verifying CEF network accounting	Configuring CEF Network Accounting
Tasks for customizing the display of recorded CEF events	Customizing the Display of Recorded CEF Events
Causes of common CEF-related error messages on platforms running dCEF 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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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.

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

dCEF—distributed Cisco Express Forwarding. A mode of CEF 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 (CEF) 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 CEF 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 (CEF) tables from the Route Switch Processor (RSP) to the line card when the router is operating in distributed CEF (dCEF) 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.

Note Refer to the Cisco *Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Configuring CEF Consistency Checkers

Table 13 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 12.0(3)S or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 13 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 13 Feature Information for Configuring CEF Consistency Checkers

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.	—	—

Configuring CEF Network Accounting

First Published: May 2, 2005
Last Updated: November 29, 2005

This module contains information about and instructions for configuring network accounting for Cisco Express Forwarding (CEF). Accounting produces the statistics that enable you to better understand CEF 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.

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Configuring CEF Network Accounting" section on page 132

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for Configuring CEF Network Accounting, page 108
- Information About Configuring CEF Network Accounting, page 108
- How to Configure CEF Network Accounting, page 115
- Configuration Examples for Configuring CEF Network Accounting, page 127
- Additional References, page 129
- Glossary, page 131
- Feature Information for Configuring CEF Network Accounting, page 132

Prerequisites for Configuring CEF Network Accounting

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

Information About Configuring CEF Network Accounting

Before you configure CEF network accounting, you should understand the following information:

- Cisco Platform Support for Central CEF and dCEF, page 108
- Traffic Matrix Statistics That You Can Collect and View, page 109
- TMS and CEF Nonrecursive Accounting in Backbone Routers, page 109
- How Backbone Routers Collect TMS, page 110
- TMS Viewing Options, page 113

For links to information about other CEF and dCEF features that you can configure, go to the "Additional References" section on page 129.

Cisco Platform Support for Central CEF and dCEF

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

To find out if CEF is enabled on your platform, enter the **show ip cef** command. If CEF 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 CEF 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 CEF (dCEF) is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When dCEF is enabled on your platform, the line cards perform the express forwarding.

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

Central CEF or dCEF has the following restrictions:

- The Cisco 12000 Series Internet routers operate only in dCEF mode. On these routers, you must not disable dCEF on an interface.
- If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are process switched. Logging disables CEF.

- dCEF switching cannot be configured on the same VIP card on which distributed fast switching is configured.
- dCEF is not supported on Cisco 7200 series routers.

See the "Additional References" section on page 129 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 CEF 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 CEF 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 CEF 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.

CEF represents IGP routes as nonrecursive entries and BGP routes as recursive entries that resolve through nonrecursive entries.

CEF nonrecursive accounting counts the packets for all of the CEF recursive entries (from BGP routes) that resolve through a CEF 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 CEF 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 CEF 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. CEF 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, CEF 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 11 and Figure 12 help illustrate the traffic statistics you can gather using TMS.

Figure 11 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 11 Sample Network with Backbone Routers and Links

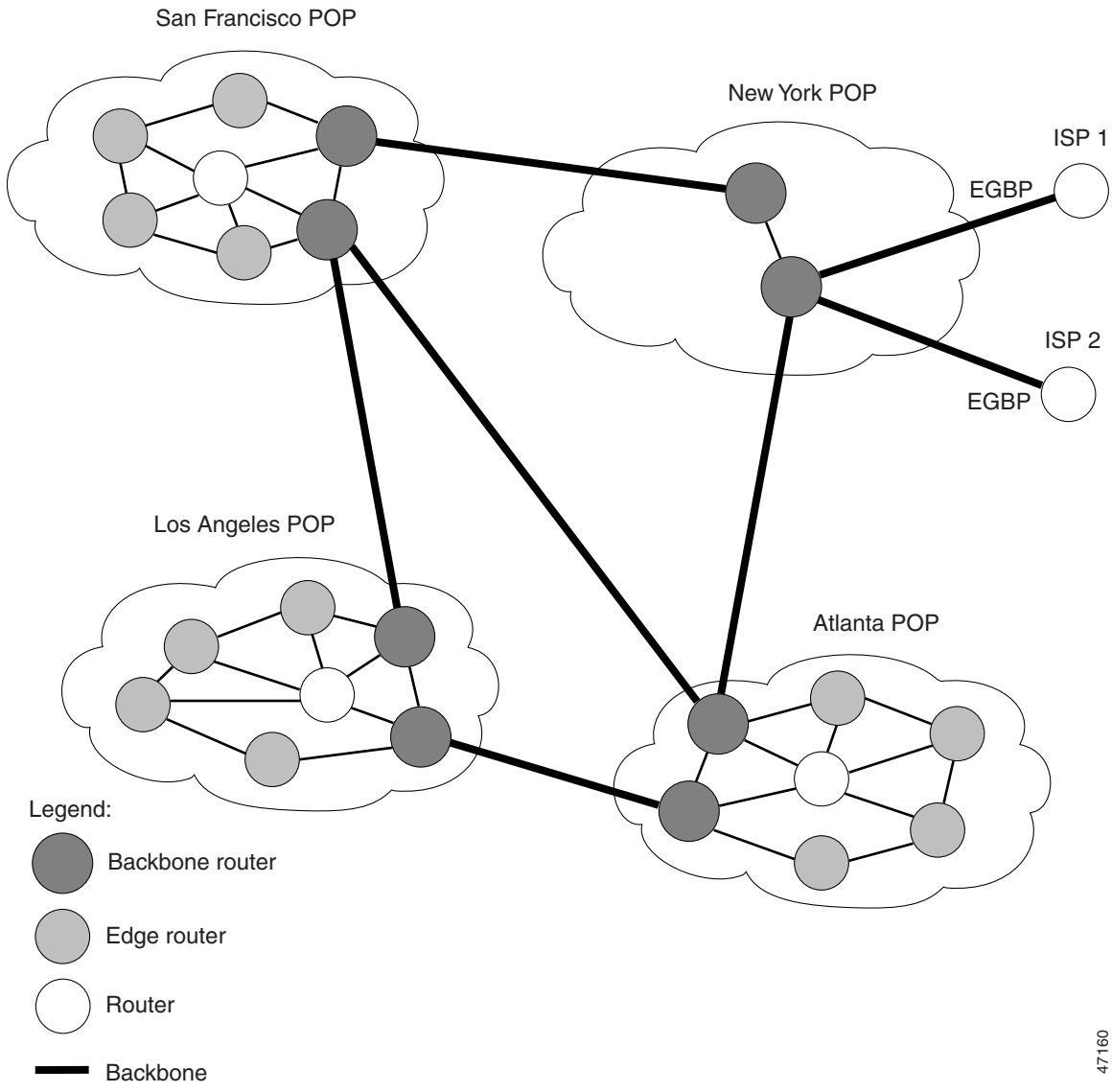
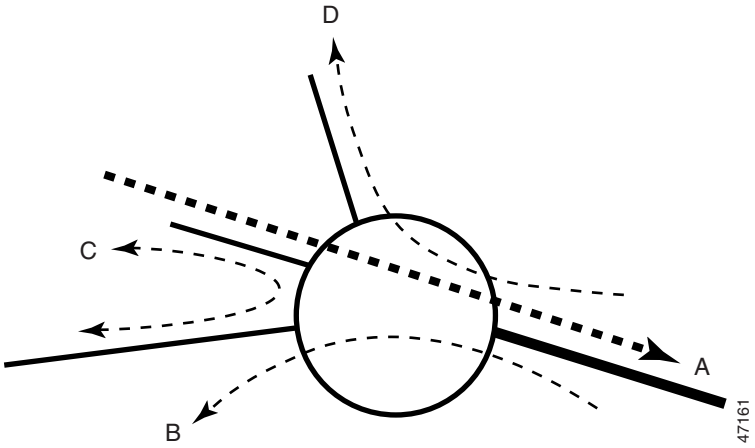


Figure 12 shows an exploded view of the backbone router that links the Los Angeles point of presence (POP) in Figure 11 to the Atlanta POP. The bold line represents the backbone link going to the Atlanta POP.

Figure 12 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 12 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 12) is the most important for determining the amount of traffic that travels through a backbone router. Internal traffic (paths B and D in Figure 12) 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:

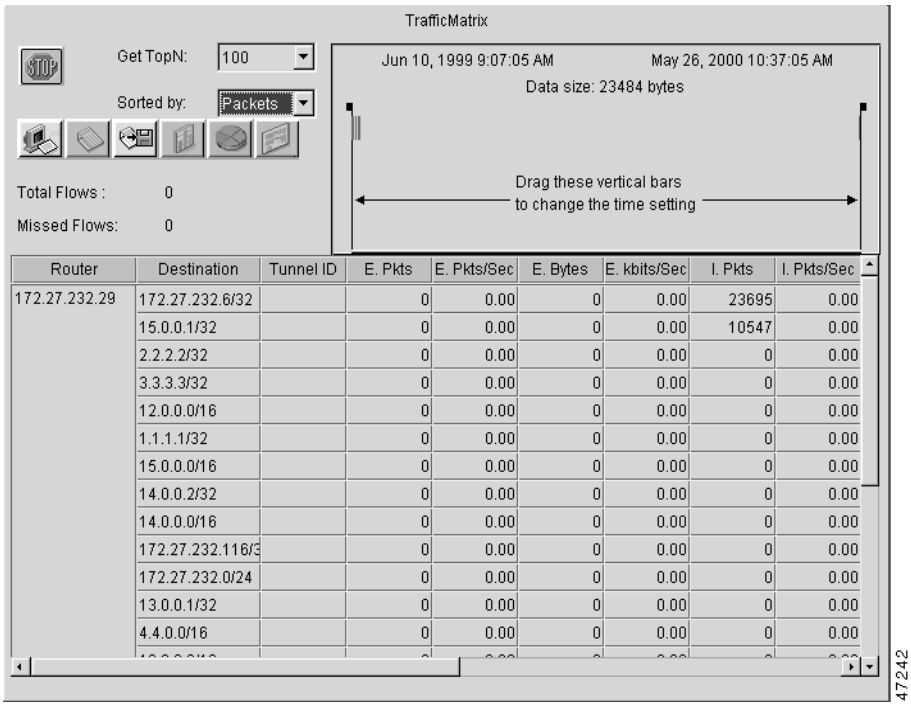
- Viewing the data in a graphical format, using the NDA Display module. The Display module is useful for graphing the traffic matrix data and comparing statistics. See the "TMS Displayed with the NDA Display Module" section on page 113 for more information.
- Entering the **more system:vfiles/tmstats_ascii** command on the backbone router. This command displays a TMS table. See the "Interpreting the Statistics in the tmstats_ascii File" section on page 121 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 114 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 13 and Figure 14. The display format depends on the aggregation scheme you select. Refer to the *Network Data Analyzer Installation and User Guide* for more information.

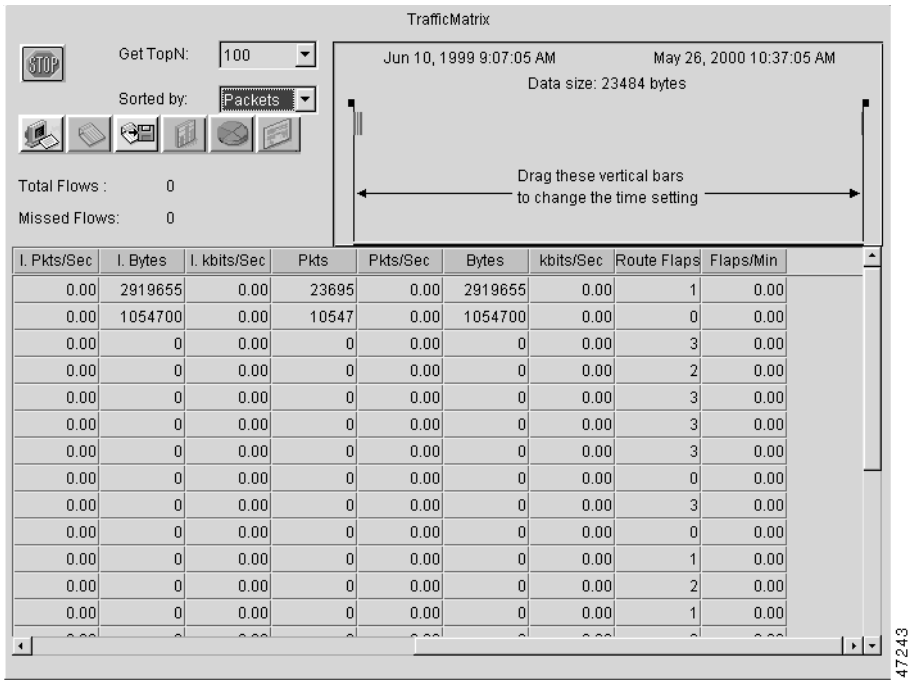
(The view of data that the NDA Display module provides is wide. Slide the scroll bar to the right and left to see all of the data. Figure 13 and Figure 14 taken together show all of the columns of data.)

Figure 13 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 14 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 CEF Network Accounting

Perform the following tasks to configure CEF network accounting:

- Configuring CEF Network Accounting, page 115 (required)
- Enabling a Backbone Router to Collect TMS, page 116 (optional)
- Interpreting the Statistics in the tmstats_ascii File, page 121 (optional)
- Viewing Information in the tmasinfo File: BGP Neighbor Autonomous Systems for IGP Destinations, page 124 (optional)
- Verifying CEF Network Accounting Information, page 126 (optional)

Configuring CEF Network Accounting

Perform the following task to enable network accounting for CEF.

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

When you enable network accounting for dCEF 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 CEF or dCEF, 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 CEF 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 CEF. 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 116 (optional)
- Enabling the NDA to Collect TMS on a Backbone Router, page 118 (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 CEF 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 CEF 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.

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.

	Command or Action	Purpose
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 UtilityServer host in the network, the Traffic Matrix Statistics Control window shown in Figure 15 appears.

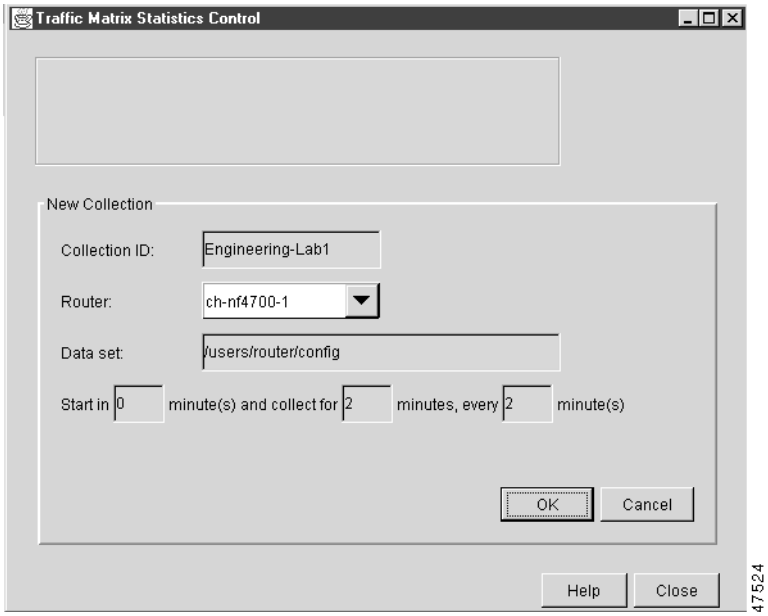
Step 3 Specify the new TMS collection parameters, using the Traffic Matrix Statistics Control window.

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 15.

Figure 15 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 16 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 16.

Figure 16 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 CEF, 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 121
- tmstats_ascii File Header Description, page 121
- Destination Prefix Record Description, page 122
- Tunnel Midpoint Record Description, page 123

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 14 describes the fields in the file header of the tmstats_ascii file.

Table 14 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 14 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 15 describes the fields in the destination prefix record.

Table 15 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 16 describes the fields in the tunnel midpoint record.

Table 16 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 121

- Destination prefix record (dynamic label switching or traffic engineering (TE) tunnel data)—"Destination Prefix Record Description" section on page 122
- Tunnel midpoint record (TE tunnel midpoint data)—"Tunnel Midpoint Record Description" section on page 123

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 124
- Neighbor AS Record in tmsasinfo File, page 125

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 17 describes the fields in the file header.

Table 17 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 18 describes the fields in the neighbor AS record.

Table 18 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 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 124.
- Neighbor AS Record—"Neighbor AS Record in tmsasinfo File" section on page 125. The file displays BGP ASs associated with each IGP destination.

Verifying CEF Network Accounting Information

Perform the following task to verify that CEF 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 CEF 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 CEF enabled. In this example, the CEF 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 CEF 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 dCEF 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 CEF 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 CEF Network Accounting

The following sections contain configuration examples for CEF accounting:

- Configuring CEF Network Accounting: Example, page 127
- Enabling a Backbone Router to Collect TMS Data: Example, page 127
- IP CEF Nonrecursive Accounting Configuration: Example, page 128
- Interpreting the Statistics in the tmstats_ascii File: Example, page 129

Configuring CEF Network Accounting: Example

The following example shows how to enable the collection of CEF 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
```

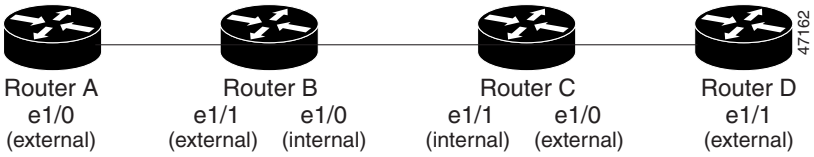
```
!
interface e1/0
 ip cef accounting non-recursive external
 end
```

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

IP CEF Nonrecursive Accounting Configuration: Example

The following example shows an IP CEF 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 17 shows the sample backbone configuration.

Figure 17 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 CEF.

Related Documents

Related Topic	Document Title
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 CEF and dCEF operation	Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks
Tasks for enabling or disabling CEF or dCEF	Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks
Tasks for configuring load-balancing schemes for CEF	Configuring a Load-Balancing Scheme for CEF Traffic
Tasks for configuring CEF consistency checkers	Configuring CEF Consistency Checkers for Route Processors and Line Cards
Tasks for configuring epochs for CEF tables	Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables
Tasks for customizing the display of recorded CEF events	Customizing the Display of Recorded CEF 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 CEF	*Cisco IOS IP Switching Command Reference*, Release 12.4

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

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

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

dCEF—distributed Cisco Express Forwarding. A type of CEF 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 (CEF). The router uses the FIB lookup table to make destination-based switching decisions during CEF 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.

Note Refer to the Cisco *Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Configuring CEF Network Accounting

Table 19 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.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 19 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 19 Feature Information for Configuring CEF 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.	—	—

Customizing the Display of Recorded CEF Events

First Published: May 2, 2005
Last Updated: May 2, 2005

This module contains information about and instructions for customizing the display of recorded Cisco Express Forwarding (CEF) events. You can customize the CEF event log display by specifying the size of the CEF event log or by choosing to display events by prefix and mask or by CEF Virtual Private Network (VPN) routing/forwarding instance (VRF).

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Customizing the Display of Recorded CEF Events" section on page 141.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- Prerequisites for Customizing the Display of Recorded CEF Events, page 134
- Restrictions for Customizing the Display of Recorded CEF Events, page 134
- Information About Customizing the Display of Recorded CEF Events, page 134
- How to Customize the Display of Recorded CEF Events, page 135

- Configuration Examples for Customizing the Display of Recorded CEF Events, page 138
- Additional References, page 138
- Glossary, page 140
- Feature Information for Customizing the Display of Recorded CEF Events, page 141

Prerequisites for Customizing the Display of Recorded CEF Events

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

Restrictions for Customizing the Display of Recorded CEF Events

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

Information About Customizing the Display of Recorded CEF Events

Before customizing CEF event logging, you should understand the following:

- Cisco Platform Support for Central CEF and dCEF, page 134
- CEF Event Log Overview, page 135

For links to information about other CEF and dCEF features that you can configure, go to the "Additional References" section on page 138.

Cisco Platform Support for Central CEF and dCEF

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

To find out if CEF is enabled on your platform, enter the **show ip cef** command. If CEF 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 CEF 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 CEF (dCEF) is enabled by default on the Catalyst 6500 series switch, the Cisco 7500 series router, and the Cisco 12000 Series Internet Router. When dCEF is enabled on your platform, the line cards perform the express forwarding.

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

CEF Event Log Overview

The CEF event log collects CEF 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 CEF feature.

When the CEF 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 CEF 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 CEF events:

- The **show ip cef events** command displays all recorded CEF forwarding information base (FIB) and adjacency events.
- The **debug ip cef** command and the **events** keyword record general CEF events as they occur.
- The **debug ip cef table** command enables the real-time collection of events that affect entries in the CEF tables.

How to Customize the Display of Recorded CEF Events

Perform the following tasks to customize CEF event logging and display logging events:

- Customizing CEF Event Logging, page 135 (optional)
- Displaying CEF Event-Log Information, page 136 (optional)

Customizing CEF Event Logging

This section contains information about and instructions for customizing CEF 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.
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 CEF 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) CEF table.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

Displaying CEF Event-Log Information

Perform the following task to display CEF 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 CEF 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 CEF 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 CEF 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 CEF 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 Customizing the Display of Recorded CEF Events

This section contains one configuration example for customizing the display of recorded CEF events: Customizing CEF Event Logging: Example, page 138

Customizing CEF Event Logging: Example

The following example shows how to enable event logging for CEF:

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

In this example, the CEF event log is configured to hold 25000 entries.

Additional References

The following sections provide references related to the customizing of the display of recorded CEF events.

Related Documents

Related Topic	Document Title
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 CEF and dCEF operation	Configuring Basic CEF for Improved Performance, Scalability, and Resiliency in Dynamic Networks
Tasks for enabling or disabling CEF or dCEF	Enabling or Disabling CEF or dCEF to Customize Switching/Forwarding for Dynamic Networks
Tasks for configuring load-balancing schemes for CEF	Configuring a Load-Balancing Scheme for CEF Traffic
Tasks for configuring CEF consistency checkers	Configuring CEF Consistency Checkers for Route Processors and Line Cards

Related Topic	Document Title
Tasks for configuring epochs for CEF tables	Configuring Epochs to Clear and Rebuild CEF and Adjacency Tables
Tasks for configuring and verifying CEF network accounting	Configuring CEF Network Accounting
Causes of common CEF-related error messages on platforms running dCEF 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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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.

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

dCEF—distributed Cisco Express Forwarding. A mode of CEF 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 (CEF) 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 CEF 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.

Note Refer to the Cisco *Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Customizing the Display of Recorded CEF Events

Table 20 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.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

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

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 20 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 20 Feature Information for Customizing the Display of Recorded CEF 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.	—	—

Cisco Systems

Part 2: Fast Switching

Configuring Fast Switching

This chapter describes how to configure fast switching on Cisco IOS devices. It provides configuration guidelines for switching paths and tuning guidelines.

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the section "Finding Additional Feature Support Information" section on page xxxiii in the chapter "Using Cisco IOS Software for Release 12.4."

Fast Switching Configuration Task List

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.

To configure fast switching, perform the tasks described in the following sections:

- Enabling AppleTalk Fast Switching
- Enabling IP Fast Switching
- Enabling Fast Switching on the Same IP Interface
- Enabling Fast Switching of IPX Directed Broadcast Packets
- Enabling SMDS Fast Switching

Fast switching is not supported for the X.25 encapsulations.

Enabling AppleTalk Fast Switching

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.

Enabling IP Fast Switching

Fast switching involves the use of a high-speed switching cache for IP routing. Destination IP addresses are stored in the high-speed cache to expedite packet forwarding. In some cases, fast switching is inappropriate, such as when slow-speed serial links (64K and below) are being fed from higher-speed media such as T1 or Ethernet. In such a case, disabling fast switching can reduce the packet drop rate to some extent. Fast switching allows outgoing packets to be load balanced on a *per-destination* basis.

To enable or disable fast switching, use the following commands in interface configuration mode:

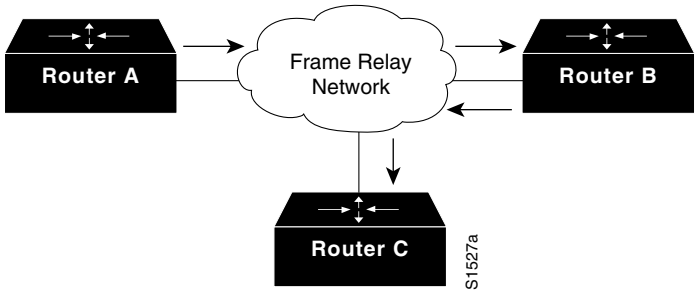
Command	Purpose
`Router(config-if)# ip route-cache`	Enables fast switching (use of a high-speed route cache for IP routing).
`Router(config-if)# no ip route-cache`	Disables fast switching and enables load balancing on a per-packet basis.

Enabling Fast Switching on the Same IP Interface

You can enable IP fast switching when the input and output interfaces are the same interface. This normally is not recommended, though it is useful when you have partially meshed media such as Frame Relay. You could use this feature on other interfaces, although it is not recommended because it would interfere with redirection.

Figure 18 illustrates a scenario where enabling fast switching on the same IP interface is desirable. Router A has a data-link connection identifier (DLCI) to Router B, and Router B has a DLCI to Router C. There is no DLCI between Routers A and C; traffic between them must go in and out of Router B through the same interface.

Figure 18 IP Fast Switching on the Same Interface



To allow IP fast switching on the same interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip route-cache same-interface`	Enables the fast switching of packets out of the same interface on which they arrived.

Enabling Fast Switching of IPX Directed Broadcast Packets

By default, Cisco IOS software switches IPX packets that have been directed to the broadcast address. To enable fast switching of these IPX-directed broadcast packets, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ipx broadcast-fastswitching`	Enables fast switching of IPX directed broadcast packets.

Enabling SMDS Fast Switching

SMDS fast switching of IP, 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.

By default, SMDS fast switching is enabled.

To reenable fast switching if it has been disabled, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# interface` *type number*	Defines the type and unit number of the interface, and enters interface configuration mode.
Step 2	`Router(config-subif)# encapsulation smds`	Sets SMDS encapsulation.
Step 3	`Router(config-if)# ip route-cache`	Enables the interface for IP fast switching.
Step 4	`Router(config-if)# ipx route-cache`	Enables the interface for IPX fast switching.
Step 5	`Router(config-if)# appletalk route-cache`	Enables the interface for AppleTalk fast switching.

Disabling Fast Switching for Troubleshooting

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 will be process switched by the system's CPU.

For some diagnostics, such as debugging and packet-level tracing, you will 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 will be 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.

To disable fast switching, perform the tasks described in the following sections:

- Disabling AppleTalk Fast Switching
- Disabling Banyan VINES Fast Switching
- Disabling DECnet Fast Switching
- Disabling IPX Fast Switching
- Disabling ISO CLNS Fast Switching Through the Cache
- Disabling XNS Fast Switching

Disabling AppleTalk Fast Switching

To disable AppleTalk fast switching on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# no appletalk route-cache`	Disables AppleTalk fast switching.

Disabling Banyan VINES Fast Switching

Fast switching is enabled by default on all interfaces on which it is supported.

To disable fast switching on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# no vines route-cache`	Disables fast switching.

Disabling DECnet Fast Switching

By default, DECnet routing software implements fast switching of DECnet packets.

To disable fast switching of DECnet packets, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# no decnet route-cache`	Disables fast switching of DECnet packets on a per-interface basis.

Disabling IPX Fast Switching

To disable IPX fast switching, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# no ipx route-cache`	Disables IPX fast switching.

Disabling ISO CLNS Fast Switching Through the Cache

ISO CLNS fast switching through the cache is enabled by default for all supported interfaces. To disable fast switching, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# no clns route-cache`	Disables fast switching.

Note The cache still exists and is used after the **no clns route-cache** interface configuration command is used; the software does not do fast switching through the cache.

Disabling XNS Fast Switching

To disable XNS fast switching on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# no xns route-cache`	Disables XNS fast switching.

Controlling the Route Cache

The high-speed route cache used by IP fast switching is invalidated when the IP routing table changes. By default, the invalidation of the cache is delayed slightly to avoid excessive CPU load while the routing table is changing. To control the route cache, perform the tasks described in the following sections:

- Controlling Route Cache Invalidation for IP
- Displaying System and Network Statistics
- Adjusting the Route Cache for IPX
- Padding Odd-Length IPX Packets

Controlling Route Cache Invalidation for IP

To control route cache invalidation, use the following commands in global configuration mode as needed for your network:

Command	Purpose
`Router(config)# no ip cache-invalidate-delay`	Allows immediate invalidation of the cache.
`Router(config)# ip cache-invalidate-delay [minimum maximum quiet threshold]`	Delays invalidation of the cache.

Caution Normally, this task should not be necessary. It should be performed only under the guidance of technical staff. Incorrect configuration can seriously degrade the performance of your router.

Displaying System and Network Statistics

You can display the contents of IP routing tables and caches. The resulting information can be used to determine resource utilization and to solve network problems.

To display system and network statistics, use the following command in privileged EXEC mode:

Command	Purpose
`Router# show ip cache [prefix mask] [type number]`	Displays the routing table cache used to fast switch IP traffic.

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 (Optional)
- Controlling IPX Route Cache Invalidation (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 set a maximum limit on the number of entries in the IPX route cache, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ipx route-cache max-size size`	Sets a maximum limit on the number of entries in the IPX route cache.

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 Invalidation" section in this chapter for more information on invalidating route cache entries.

Controlling IPX Route Cache 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 configure the router to invalidate fast-switch cache entries that are inactive, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ipx route-cache inactivity-timeout period [rate]`	Invalidates fast switch cache entries that are inactive.

When you use the **ipx route-cache inactivity-timeout** command with the **ipx route-cache max-size** global configuration command, you can ensure a small route cache with fresh entries.

Padding 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.

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, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# no ipx route-cache`	Disables fast switching.
Step 2	`Router(config-if)# ipx pad-process-switched-packets`	Enables the padding of odd-length packets.

Part 3: Multicast Distributed Switching

Configuring Multicast Distributed Switching

This chapter describes the required and optional tasks for configuring Multicast Distributed Switching (MDS).

For a complete description of the commands in this chapter, refer to the the *Cisco IOS Switching Services Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the section Finding Additional Feature Support Information in the chapter Using Cisco IOS Software for Release 12.4.

Prior to multicast distributed switching, IP multicast traffic was always switched at the Route Processor (RP) in the Route Switch Processor (RSP)-based platforms. Starting with Cisco IOS Release 11.2 GS, IP multicast traffic can be distributed switched on RSP-based platforms with VIPs. Furthermore, MDS is the only multicast switching method on the Cisco 12000 Gigabit Switch Router (GSR), starting with Cisco IOS Release 11.2(11)GS.

Switching multicast traffic at the RP had the following disadvantages:

- The load on the RP increased. This affected important route updates and calculations (for 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 (VIPs in the case of RSP, and line cards in the case of GSR). The line card is the interface card that houses the VIPs (in the case of RSP) and the GSR line card (in the case of GSR). 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.

In the case of RSP, packets received on non-VIP IPs are switched by the RP.

MDS can work in conjunction with Cisco Express Forwarding (CEF), unicast distributed fast switching (DFS), or flow switching.

MDS Configuration Task List

To configure MDS, perform the task described in the following sections. The first section contains a required task; the remaining task is optional:

- Enabling MDS (Required)
- Monitoring and Maintaining MDS (Optional)

Enabling MDS

To enable MDS, you must enable it globally and on at least one interface because MDS is an attribute of the interface. Use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip multicast-routing distributed`	Enables MDS globally.
Step 2	`Router(config)# interface type number`	Configures an interface.
Step 3	`Router(config-if)# ip route-cache distributed`	Enables distributed switching on the RSP. (This step is required on the RSP platform only.)
Step 4	`Router(config-if)# ip mroute-cache distributed`	Enables MDS on the interface.
	Repeat Steps 2 through 4 for each interface that you want to perform MDS.	

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.

Monitoring and Maintaining MDS

To maintain MDS on the line cards, use the following command in EXEC mode:

Command	Purpose
`Router# clear ip mds forwarding`	Clears the MFIB table of the line card and resynchronizes with the RP.

To maintain MDS on the RP, use the following commands in EXEC mode, as needed:

Command	Purpose
`Router# clear ip mroute {* | group [source]}`	Clears multicast routes and counts.
`Router# clear ip pim interface count`	Clears all packet counts on the line cards.

To monitor MDS on the line cards, use the following commands in EXEC mode, as needed. Remember that to reach a line card's console, enter the **attach** *slot#* command, using the slot number where the line card resides.

Command	Purpose
`Router# show ip mds forwarding [group-address] [source-address]`	Displays the MFIB table, forwarding information, related flags, and counts.
`Router# show ip mds summary`	Displays a summary of the MFIB.

To monitor MDS on the RP, use the following commands in EXEC mode, as needed:

Command	Purpose
`Router# show ip mds stats [switching | linecard]`	Displays switching statistics or line card statistics for MDS.
`Router# show ip mds interface`	Displays the status of MDS interfaces.
`Router# show ip pim interface [type number] count`	Displays switching counts for unicast distributed fast switching and other fast switching statistics.
`Router# show ip mcache [group [source]]`	Displays the contents of the IP fast-switching cache.
`Router# show interface stats`	Displays numbers of packets that were process switched, fast switched, and distributed switched.

MDS Configuration Example

The following example enables MDS. The **ip route-cache distributed** interface configuration command is needed on the RSP only, not on the GSR.

```
ip multicast-routing distributed
 interface pos 1/0/0
 ip route-cache distributed
 ip mroute-cache distributed
```