Cisco IOS IP Routing: EIGRP Configuration Guide

12.4
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

All Cisco product names, trademarks, logos, and services are the property of Cisco Systems, Inc. and its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

Cisco IOS IP Routing: EIGRP Configuration Guide, Release 12.4
© 2009 Cisco Systems, Inc. All rights reserved.
About Cisco IOS Software Documentation

Last Updated: October 14, 2009

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

- Documentation Objectives, page i
- Audience, page i
- Documentation Conventions, page i
- Documentation Organization, page iii
- Additional Resources and Documentation Feedback, page xii

Documentation Objectives

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

Audience

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

Documentation Conventions

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

Cisco IOS documentation uses the following typographic conventions:

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

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bold</td>
<td>Bold text indicates commands and keywords that you enter as shown.</td>
</tr>
<tr>
<td>italic</td>
<td>Italic text indicates arguments for which you supply values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional keyword or argument.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
</tbody>
</table>
Software Conventions

Cisco IOS software uses the following program code conventions:

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

Reader Alert Conventions

Cisco IOS documentation uses the following conventions for reader alerts:

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

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

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

Documentation Organization

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

- Cisco IOS Documentation Set, page iv
- Cisco IOS Documentation on Cisco.com, page iv
- Configuration Guides, Command References, and Supplementary Resources, page v
Cisco IOS Documentation Set

The Cisco IOS documentation set consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether updates have been made to a feature.

- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.

- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.

- Command reference book for debug commands. Command pages are listed in alphabetical order.

- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

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

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

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

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

Configuration Guides

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

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

Cisco IOS Supplementary Documents and Resources

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

Configuration Guides, Command References, and Supplementary Resources

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

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

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

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

Table 1  Cisco IOS Configuration Guides and Command References

<table>
<thead>
<tr>
<th>Configuration Guide and Command Reference Titles</th>
<th>Features/Protocols/Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco IOS AppleTalk Configuration Guide</td>
<td>AppleTalk protocol.</td>
</tr>
<tr>
<td>• Cisco IOS AppleTalk Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS Asynchronous Transfer Mode Configuration Guide</td>
<td>LAND ATM, multiprotocol over ATM (MPoA), and WAN ATM.</td>
</tr>
<tr>
<td>• Cisco IOS Asynchronous Transfer Mode Command Reference</td>
<td></td>
</tr>
<tr>
<td>Configuration Guide and Command Reference Titles</td>
<td>Features/Protocols/Technologies</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Cisco IOS Bridging and IBM Networking Configuration Guide</td>
<td>Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRRSM).</td>
</tr>
<tr>
<td>• Cisco IOS Bridging Command Reference</td>
<td>Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.</td>
</tr>
<tr>
<td>• Cisco IOS IBM Networking Command Reference</td>
<td>PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).</td>
</tr>
<tr>
<td>• Cisco IOS Broadband Access Aggregation and DSL Configuration Guide</td>
<td>Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and Operation, Administration, and Maintenance (OAM).</td>
</tr>
<tr>
<td>• Cisco IOS Carrier Ethernet Configuration Guide</td>
<td>Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.</td>
</tr>
<tr>
<td>• Cisco IOS Configuration Fundamentals Configuration Guide</td>
<td>DECnet protocol.</td>
</tr>
<tr>
<td>• Cisco IOS Configuration Fundamentals Command Reference</td>
<td>Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).</td>
</tr>
<tr>
<td>• Cisco IOS DECnet Configuration Guide</td>
<td>Flexible NetFlow.</td>
</tr>
<tr>
<td>• Cisco IOS DECnet Command Reference</td>
<td>A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.</td>
</tr>
<tr>
<td>• Cisco IOS Integrated Session Border Controller Command Reference</td>
<td>A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).</td>
</tr>
<tr>
<td>Configuration Guide and Command Reference Titles</td>
<td>Features/Protocols/Technologies</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>• Cisco IOS Intelligent Services Gateway</td>
<td>Subscriber identification,</td>
</tr>
<tr>
<td>Configuration Guide</td>
<td>service and policy determination,</td>
</tr>
<tr>
<td>• Cisco IOS Intelligent Services Gateway</td>
<td>session creation, session</td>
</tr>
<tr>
<td>Command Reference</td>
<td>policy enforcement, session</td>
</tr>
<tr>
<td></td>
<td>life-cycle management,</td>
</tr>
<tr>
<td></td>
<td>accounting for access and service</td>
</tr>
<tr>
<td></td>
<td>usage, and session state</td>
</tr>
<tr>
<td></td>
<td>monitoring.</td>
</tr>
<tr>
<td>• Cisco IOS Interface and Hardware Component</td>
<td>LAN interfaces, logical</td>
</tr>
<tr>
<td>Configuration Guide</td>
<td>interfaces, serial interfaces,</td>
</tr>
<tr>
<td>• Cisco IOS Interface and Hardware Component</td>
<td>virtual interfaces, and</td>
</tr>
<tr>
<td>Command Reference</td>
<td>interface configuration.</td>
</tr>
<tr>
<td>• Cisco IOS IP Addressing Services</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>Configuration Guide</td>
<td>(ARP), Network Address</td>
</tr>
<tr>
<td>• Cisco IOS IP Addressing Services</td>
<td>Translation (NAT), Domain Name</td>
</tr>
<tr>
<td>Command Reference</td>
<td>System (DNS), Dynamic</td>
</tr>
<tr>
<td></td>
<td>Host Configuration Protocol</td>
</tr>
<tr>
<td></td>
<td>(DHCP), and Next Hop Address</td>
</tr>
<tr>
<td></td>
<td>Resolution Protocol (NHRP).</td>
</tr>
<tr>
<td>• Cisco IOS IP Application Services</td>
<td>Enhanced Object Tracking (EOT),</td>
</tr>
<tr>
<td>Configuration Guide</td>
<td>Gateway Load Balancing Protocol</td>
</tr>
<tr>
<td>• Cisco IOS IP Application Services</td>
<td>(GLBP), Hot Standby Router</td>
</tr>
<tr>
<td>Command Reference</td>
<td>Protocol (HSRP), IP Services,</td>
</tr>
<tr>
<td></td>
<td>Server Load Balancing (SLB),</td>
</tr>
<tr>
<td></td>
<td>Stream Control Transmission</td>
</tr>
<tr>
<td></td>
<td>Protocol (SCTP), TCP, Web Cache</td>
</tr>
<tr>
<td></td>
<td>Communication Protocol (WCCP),</td>
</tr>
<tr>
<td></td>
<td>User Datagram Protocol (UDP),</td>
</tr>
<tr>
<td></td>
<td>and Virtual Router Redundancy</td>
</tr>
<tr>
<td></td>
<td>Protocol (VRRP).</td>
</tr>
<tr>
<td>• Cisco IOS IP Mobility Configuration Guide</td>
<td>Mobile ad hoc networks (MANet)</td>
</tr>
<tr>
<td>• Cisco IOS IP Mobility Command Reference</td>
<td>and Cisco mobile networks.</td>
</tr>
<tr>
<td>• Cisco IOS IP Multicast Configuration Guide</td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td>• Cisco IOS IP Multicast Command Reference</td>
<td>(PIM) sparse mode (PIM-SM),</td>
</tr>
<tr>
<td></td>
<td>bidirectional PIM (bidir-PIM),</td>
</tr>
<tr>
<td></td>
<td>Source Specific Multicast</td>
</tr>
<tr>
<td></td>
<td>(SSM), Multicast Source</td>
</tr>
<tr>
<td></td>
<td>Discovery Protocol (MSDP),</td>
</tr>
<tr>
<td></td>
<td>Internet Group Management</td>
</tr>
<tr>
<td></td>
<td>Protocol (IGMP), and Multicast</td>
</tr>
<tr>
<td></td>
<td>VPN (MVPN).</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing Protocols Configuration</td>
<td>Border Gateway Protocol (BGP),</td>
</tr>
<tr>
<td>Guide</td>
<td>multiprotocol BGP, multiprotocol</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing Protocols Command</td>
<td>BGP extensions for IP multicast,</td>
</tr>
<tr>
<td>Reference</td>
<td>bidirectional forwarding</td>
</tr>
<tr>
<td></td>
<td>detection (BFD), Enhanced</td>
</tr>
<tr>
<td></td>
<td>Interior Gateway Routing</td>
</tr>
<tr>
<td></td>
<td>Protocol (EIGRP), Interior</td>
</tr>
<tr>
<td></td>
<td>Gateway Routing Protocol (IGRP),</td>
</tr>
<tr>
<td></td>
<td>Intermediate System-to-</td>
</tr>
<tr>
<td></td>
<td>Intermediate System (IS-IS),</td>
</tr>
<tr>
<td></td>
<td>On-Demand Routing (ODR), Open</td>
</tr>
<tr>
<td></td>
<td>Shortest Path First (OSPF),</td>
</tr>
<tr>
<td></td>
<td>and Routing Information</td>
</tr>
<tr>
<td></td>
<td>Protocol (RIP).</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: BFD Configuration Guide</td>
<td>Bidirectional forwarding</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: BGP Configuration</td>
<td>detection (BFD).</td>
</tr>
<tr>
<td>Guide</td>
<td>Border Gateway Protocol (BGP),</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: BGP Command Reference</td>
<td>multiprotocol BGP, multiprotocol</td>
</tr>
<tr>
<td></td>
<td>BGP extensions for IP multicast,</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: EIGRP Configuration</td>
<td>Enhanced Interior Gateway</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: EIGRP Command Reference</td>
<td>Intermediate System-to-</td>
</tr>
<tr>
<td></td>
<td>Intermediate System (IS-IS).</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: ISIS Configuration</td>
<td>On-Demand Routing (ODR).</td>
</tr>
<tr>
<td>Guide</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: ISIS Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: ODR Configuration Guide</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: ODR Command Reference</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1  
**Cisco IOS Configuration Guides and Command References (continued)**

<table>
<thead>
<tr>
<th>Configuration Guide and Command Reference Titles</th>
<th>Features/Protocols/Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco IOS IP Routing: OSPF Configuration Guide</td>
<td>Open Shortest Path First (OSPF).</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: OSPF Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: Protocol-Independent Configuration Guide</td>
<td>IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.</td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: Protocol-Independent Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS IP Routing: RIP Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS IP SLAs Configuration Guide</td>
<td>Cisco IOS IP Service Level Agreements (IP SLAs).</td>
</tr>
<tr>
<td>• Cisco IOS IP SLAs Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS IP Switching Configuration Guide</td>
<td>Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).</td>
</tr>
<tr>
<td>• Cisco IOS IP Switching Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS IPv6 Configuration Guide</td>
<td>For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document.</td>
</tr>
<tr>
<td>• Cisco IOS IPv6 Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS ISO CLNS Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS LAN Switching Configuration Guide</td>
<td>VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).</td>
</tr>
<tr>
<td>• Cisco IOS LAN Switching Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</td>
<td>Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.</td>
</tr>
<tr>
<td>• Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS Mobile Wireless Home Agent Configuration Guide</td>
<td>Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.</td>
</tr>
<tr>
<td>• Cisco IOS Mobile Wireless Home Agent Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</td>
<td>Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.</td>
</tr>
<tr>
<td>• Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS Mobile Wireless Radio Access Networking Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS Multiprotocol Label Switching Configuration Guide</td>
<td>MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.</td>
</tr>
<tr>
<td>• Cisco IOS Multiprotocol Label Switching Command Reference</td>
<td></td>
</tr>
<tr>
<td>Configuration Guide and Command Reference Titles</td>
<td>Features/Protocols/Technologies</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>- Cisco IOS Multi-Topology Routing Configuration Guide</td>
<td>Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.</td>
</tr>
<tr>
<td>- Cisco IOS Multi-Topology Routing Command Reference</td>
<td></td>
</tr>
<tr>
<td>- Cisco IOS NetFlow Configuration Guide</td>
<td>Network traffic data analysis, aggregation caches, and export features.</td>
</tr>
<tr>
<td>- Cisco IOS NetFlow Command Reference</td>
<td></td>
</tr>
<tr>
<td>- Cisco IOS Network Management Configuration Guide</td>
<td>Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration).</td>
</tr>
<tr>
<td>- Cisco IOS Network Management Command Reference</td>
<td></td>
</tr>
<tr>
<td>- Cisco IOS Novell IPX Command Reference</td>
<td></td>
</tr>
<tr>
<td>- Cisco IOS Optimized Edge Routing Configuration Guide</td>
<td>Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks.</td>
</tr>
<tr>
<td>- Cisco IOS Optimized Edge Routing Command Reference</td>
<td></td>
</tr>
<tr>
<td>- Cisco IOS Quality of Service Solutions Configuration Guide</td>
<td>Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).</td>
</tr>
<tr>
<td>- Cisco IOS Quality of Service Solutions Command Reference</td>
<td></td>
</tr>
<tr>
<td>- Cisco IOS Security Command Reference</td>
<td>Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS++; terminal access security; and traffic filters.</td>
</tr>
<tr>
<td>- Cisco IOS Security Configuration Guide: Securing the Data Plane</td>
<td>Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching: Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.</td>
</tr>
<tr>
<td>- Cisco IOS Security Configuration Guide: Securing User Services</td>
<td>AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.</td>
</tr>
<tr>
<td>Configuration Guide and Command Reference Titles</td>
<td>Features/Protocols/Technologies</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Security Configuration Guide: Secure Connectivity</strong></td>
<td>Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Service Advertisement Framework Configuration Guide</strong></td>
<td>Cisco Service Advertisement Framework.</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Service Advertisement Framework Command Reference</strong></td>
<td>Subscriber authentication, service access, and accounting.</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Service Selection Gateway Configuration Guide</strong></td>
<td>An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Service Selection Gateway Command Reference</strong></td>
<td>Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes, and patches.</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Terminal Services Configuration Guide</strong></td>
<td>DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Terminal Services Command Reference</strong></td>
<td>Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Virtual Switch Command Reference</strong></td>
<td>Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy; L2TP extended failover; L2TP security VPDN; multihop by Dialed Number Identification Service (DNIS); timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F); RADIUS Attribute 82 (tunnel assignment ID); shell-based authentication of VPDN users; tunnel authentication via RADIUS on tunnel terminator.</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Voice Configuration Library</strong></td>
<td>Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.</td>
</tr>
<tr>
<td>• <strong>Cisco IOS Voice Command Reference</strong></td>
<td>For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.</td>
</tr>
</tbody>
</table>
Table 1  Cisco IOS Configuration Guides and Command References (continued)

<table>
<thead>
<tr>
<th>Configuration Guide and Command Reference Titles</th>
<th>Features/Protocols/Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco IOS Wide-Area Networking Configuration Guide</td>
<td>Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.</td>
</tr>
<tr>
<td>• Cisco IOS Wide-Area Networking Command Reference</td>
<td></td>
</tr>
<tr>
<td>• Cisco IOS Wireless LAN Configuration Guide</td>
<td>Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).</td>
</tr>
<tr>
<td>• Cisco IOS Wireless LAN Command Reference</td>
<td></td>
</tr>
</tbody>
</table>

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

Table 2  Cisco IOS Supplementary Documents and Resources

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

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

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

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.
Using the Command-Line Interface in Cisco IOS Software

Last Updated: October 14, 2009

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

- Initially Configuring a Device, page i
- Using the CLI, page ii
- Saving Changes to a Configuration, page xi
- Additional Information, page xii

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

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

Initially Configuring a Device

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

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

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

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

Note

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

Using the CLI

This section describes the following topics:

- Understanding Command Modes, page ii
- Using the Interactive Help Feature, page v
- Understanding Command Syntax, page vi
- Understanding Enable and Enable Secret Passwords, page vii
- Using the Command History Feature, page viii
- Abbreviating Commands, page ix
- Using Aliases for CLI Commands, page ix
- Using the no and default Forms of Commands, page x
- Using the debug Command, page x
- Filtering Output Using Output Modifiers, page x
- Understanding CLI Error Messages, page xi

Understanding Command Modes

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

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

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

Using the CLI

ROM monitor From privileged EXEC mode, issue the `reload` command. Press the Break key during the first 60 seconds while the system is booting.

- The # symbol represents the line number and increments at each prompt.
- Issue the `continue` command.

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

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

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

rommon 2 >
```

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

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

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

**Using the Interactive Help Feature**

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Provides a brief description of the Help feature in any command mode.</td>
</tr>
<tr>
<td>?</td>
<td>Lists all commands available for a particular command mode.</td>
</tr>
<tr>
<td>partial command?</td>
<td>Provides a list of commands that begin with the character string (no space between the command and the question mark).</td>
</tr>
<tr>
<td>partial command&lt;Tab&gt;</td>
<td>Completes a partial command name (no space between the command and &lt;Tab&gt;).</td>
</tr>
<tr>
<td>command ?</td>
<td>Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).</td>
</tr>
<tr>
<td>command keyword ?</td>
<td>Lists the arguments that are associated with the keyword (space between the keyword and the question mark).</td>
</tr>
</tbody>
</table>
The following examples show how to use the help commands:

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

Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

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

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

partial command-<Tab>
Router(config)# we<Tab> webvpn
```

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

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

Understanding Command Syntax

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

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.
The following examples show syntax conventions:

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

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

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

### Understanding Enable and Enable Secret Passwords

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

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

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

Note

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

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

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


Using the Command History Feature

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

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

Router# terminal history size num

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

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

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

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

Note

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

- Issue the show history command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the terminal history size and history commands.
The command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

### Abbreviating Commands

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

### Using Aliases for CLI Commands

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

Table 4 shows the default command aliases.

<table>
<thead>
<tr>
<th>Command Alias</th>
<th>Original Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>h</td>
<td>help</td>
</tr>
<tr>
<td>lo</td>
<td>logout</td>
</tr>
<tr>
<td>p</td>
<td>ping</td>
</tr>
<tr>
<td>s</td>
<td>show</td>
</tr>
<tr>
<td>u or un</td>
<td>undebug</td>
</tr>
<tr>
<td>w</td>
<td>where</td>
</tr>
</tbody>
</table>

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

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

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

Using the no and default Forms of Commands

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

Configuration commands may also have a default form, which returns the command settings to their default values. For commands that are disabled by default, using the default form has the same effect as using the no form of the command. For commands that are enabled by default and have default settings, the default form enables the command and returns the settings to their default values.

The no form is documented in the command pages of command references. The default form is generally documented in the command pages only when the default form performs a different function than the plain and no forms of the command. To see what default commands are available on your system, enter default ? in the appropriate command mode.

Using the debug Command

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


Caution

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

Filtering Output Using Output Modifiers

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

The following three output modifiers are available:

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

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.
The following example illustrates how to filter output of the `show interface` command to display only lines that include the expression “protocol.”

Router# `show interface | include protocol`

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

### Understanding CLI Error Messages

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

#### Table 5  Common CLI Error Messages

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

For more system error messages, see the following document:

- *Cisco IOS Release 12.4T System Message Guide*

### Saving Changes to a Configuration

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

Router# `copy running-config startup-config`

Destination filename [startup-config]?

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

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

Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the Cisco IOS Configuration Fundamentals Configuration Guide
- Cisco Product/Technology Support
- Support area on Cisco.com (also search for documentation by task or product)
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)
- Output Interpreter, a troubleshooting tool that analyzes command output of supported show commands
  [https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl](https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl)

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2008–2009 Cisco Systems, Inc. All rights reserved.
Configuring EIGRP

First Published: 2005
Last Updated: October 2, 2009

Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of the IGRP developed by Cisco. The convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP and IGRP is now obsolete.

The convergence technology is based on research conducted at SRI International and employs an algorithm referred to as the Diffusing Update Algorithm (DUAL). This algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for EIGRP” section on page 66.

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

Contents

• Information About EIGRP, page 2
• How to Configure EIGRP, page 16
• Configuration Examples for EIGRP, page 54
• Additional References, page 64
• Feature Information for EIGRP, page 66
Information About EIGRP

To configure EIGRP, you should understand the following concepts:

- EIGRP Features, page 2
- EIGRP Autonomous System Configuration, page 3
- EIGRP Named Configuration, page 3
- EIGRP Neighbor Relationship Maintenance, page 3
- DUAL Finite State Machine, page 4
- Protocol-Dependent Modules, page 4
- EIGRP Metric Weights, page 4
- Goodbye Message, page 5
- EIGRP Cost Metrics, page 6
- Routing Metric Offset Lists, page 6
- EIGRP Cost Metrics, page 6
- Route Summarization, page 8
- Summary Aggregate Addresses, page 8
- Floating Summary Routes, page 8
- EIGRP Route Authentication, page 10
- Hello Packets and the Hold-Time Intervals, page 11
- Split Horizon, page 11
- Link Bandwidth Percentage, page 11
- EIGRP Stub Routing, page 12
- EIGRP Stub Routing Leak Map Support, page 16

EIGRP Features

EIGRP provides the following features:

- Increased network width—With IP Routing Information Protocol (RIP), the largest possible width of your network is 15 hops. When EIGRP is enabled, the largest possible width is increased to 100 hops, and the EIGRP metric is large enough to support thousands of hops.
- Fast convergence—The DUAL algorithm allows routing information to converge quickly.
- Partial updates—EIGRP sends incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table. This feature minimizes the bandwidth required for EIGRP packets.
- Neighbor discovery mechanism—This is a simple hello mechanism used to learn about neighboring routers. It is protocol-independent.
- Variable-length subnet masks (VLSMs).
- Arbitrary route summarization.
- Scaling—EIGRP scales to large networks.
EIGRP Autonomous System Configuration

Configuring the router eigrp command with the autonomous-system-number argument creates an EIGRP configuration referred to as autonomous system configuration. EIGRP autonomous system configuration creates an EIGRP routing instance that can be used for exchanging routing information.

In EIGRP autonomous system configuration, EIGRP Virtual Private Networks (VPNs) can be configured only under IPv4 address family configuration mode. A virtual routing and forwarding instance (VRF) and route distinguisher must be defined before the address family session can be created.

It is recommended that you configure an autonomous system number when the address family is configured, either by entering the autonomous-system-number argument with the address-family command or separately using the autonomous-system command.

EIGRP Named Configuration

Configuring the router eigrp command with the virtual-instance-name argument creates an EIGRP configuration referred to as EIGRP named configuration. An EIGRP named configuration does not create an EIGRP routing instance by itself. EIGRP named configuration is a base configuration that is required to define address-family configurations under it that are used for routing.

In EIGRP named configuration, EIGRP VPNs can be configured in IPv4 and IPv6 named configurations. A virtual routing and forwarding instance (VRF) and a route distinguisher may or may not be used to create the address family.

If a VRF is not used in creating the address family, the EIGRP VPN instance assumes role of default route distinguisher and will communicate with the default route distinguisher of other routers in the same network.

EIGRP VPNs can be configured under EIGRP named configurations. A VRF and route distinguisher must be defined before the address family session can be created.

A single EIGRP routing process can support multiple VRFs. The number of VRFs that can be configured is limited only by available system resources on the router, which is determined by the number of VRFs, running processes, and available memory. However, only a single VRF can be supported by each VPN, and redistribution between different VRFs is not supported.

EIGRP Neighbor Relationship Maintenance

Neighbor relationship maintenance is the process that routers use to dynamically learn of other routers on their directly attached networks. Routers must also discover when their neighbors become unreachable or inoperative. Neighbor relationship maintenance is achieved with low overhead by routers periodically sending small hello packets. As long as hello packets are received, the Cisco IOS software can determine that a neighbor is alive and functioning. Once this status is determined, the neighboring routers can exchange routing information.

The reliable transport protocol is responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors. It supports intermixed transmission of multicast and unicast packets. Some EIGRP packets must be sent reliably and others need not be. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities (such as Ethernet) it is not necessary to send hello packets reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello with an indication in the packet informing the receivers that the packet need not be acknowledged. Other types of packets (such as updates) require acknowledgment, which is indicated in...
the packet. The reliable transport has a provision to send multicast packets quickly when unacknowledged packets are pending. This provision helps to ensure that convergence time remains low in the presence of varying speed links.

**DUAL Finite State Machine**

The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses the distance information (known as a metric) to select efficient, loop-free paths. DUAL selects routes to be inserted into a routing table based on feasible successors. A successor is a neighboring router used for packet forwarding that has a least-cost path to a destination that is guaranteed not to be part of a routing loop. When there are no feasible successors but there are neighbors advertising the destination, a recomputation must occur. This is the process whereby a new successor is determined. The amount of time required to recompute the route affects the convergence time. Recomputation is processor-intensive; it is advantageous to avoid unneeded recomputation. When a topology change occurs, DUAL will test for feasible successors. If there are feasible successors, DUAL will use any feasible successors it finds in order to avoid unnecessary recomputation.

**Protocol-Dependent Modules**

The protocol-dependent modules are responsible for network-layer protocol-specific tasks. An example is the EIGRP module, which is responsible for sending and receiving EIGRP packets that are encapsulated in IP. It is also responsible for parsing EIGRP packets and informing DUAL of the new information received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IP routing table. Also, EIGRP is responsible for redistributing routes learned by other IP routing protocols.

**EIGRP Metric Weights**

EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics. You can use the `metric weights (EIGRP)` command to adjust the default behavior of EIGRP routing and metric computations. For example, this adjustment allows you to tune system behavior to allow for satellite transmission. EIGRP metric defaults have been carefully selected to provide optimal performance in most networks.

*Note*

Adjusting EIGRP metric weights can dramatically affect network performance. Because of the complexity of this task, we recommend that you do not change the default values without guidance from an experienced network designer.

By default, the EIGRP composite metric is a 32-bit quantity that is a sum of the segment delays and the lowest segment bandwidth (scaled and inverted) for a given route. The formula used to scale and invert the bandwidth value is \(10^7/\text{minimum Bw in kilobits per second}\).

For a network of homogeneous media, this metric reduces to a hop count. For a network of mixed media (FDDI, Ethernet, and serial lines running from 9600 bits per second to T1 rates), the route with the lowest metric reflects the most desirable path to a destination.
Mismatched K Values

EIGRP K values are the metrics that EIGRP uses to calculate routes. Mismatched K values (EIGRP metrics) can prevent neighbor relationships from being established and can negatively impact network convergence. The following example explains this behavior between two EIGRP peers (ROUTER-A and ROUTER-B).

The following configuration is applied to ROUTER-A. The K values are changed with the metric weights command. A value of 2 is entered for the \texttt{k1} argument to adjust the bandwidth calculation. The value of 1 is entered for the \texttt{k3} argument to adjust the delay calculation.

```
hostname ROUTER-A
interface serial 0
  ip address 10.1.1.1 255.255.255.0
exit
router eigrp virtual-name1
  address-family ipv4 autonomous-system 4533
  network 10.1.1.0 0.0.0.255
  metric weights 0 2 0 1 0 0
```

The following configuration is applied to ROUTER-B. However, the metric weights command is not applied and the default K values are used. The default K values are 1, 0, 1, 0, and 0.

```
hostname ROUTER-B
interface serial 0
  ip address 10.1.1.2 255.255.255.0
exit
router eigrp virtual-name1
  address-family ipv4 autonomous-system 4533
  network 10.1.1.0 0.0.0.255
```

The bandwidth calculation is set to 2 on ROUTER-A and set to 1 (by default) on ROUTER-B. This configuration prevents these peers from forming a neighbor relationship.

The following error message is displayed in the console of ROUTER-B because the K values are mismatched:

```
*Apr 26 13:48:41.811: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down: K-value mismatch
```

There are two scenarios where this error message can be displayed:

- The two routers are connected on the same link and configured to establish a neighbor relationship. However, each router is configured with different K values.
- The K-value mismatch error message can also be displayed if one of the two peers has transmitted a “goodbye” message, and the receiving router does not support this message. In this case, the receiving router will interpret this message as a K-value mismatch.

Goodbye Message

The goodbye message is a feature designed to improve EIGRP network convergence. The goodbye message is broadcast when an EIGRP routing process is shut down to inform adjacent peers about the impending topology change. This feature allows supporting EIGRP peers to synchronize and recalculate neighbor relationships more efficiently than would occur if the peers discovered the topology change after the hold timer expired.
The goodbye message is supported in Cisco IOS Release 12.3(2), 12.3(2)T, and later releases. The following message is displayed by routers that run a supported release when a goodbye message is received:

*Apr 26 13:48:42.523: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down: Interface Goodbye received

A Cisco router that runs a software release that does not support the goodbye message can misinterpret the message as a K-value mismatch and display the following message:

*Apr 26 13:48:41.811: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down: K-value mismatch

**Note**
The receipt of a goodbye message by a nonsupporting peer does not disrupt normal network operation. The nonsupporting peer will terminate the session when the hold timer expires. The sending and receiving routers will reconverge normally after the sender reloads.

### Routing Metric Offset Lists

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via EIGRP. An offset list provides a local mechanism for increasing the value of routing metrics. Optionally, you can limit the offset list with either an access list or an interface.

**Note**
Offset lists are available only in IPv4 configurations. IPv6 configurations do not support offset lists.

### EIGRP Cost Metrics

EIGRP receives dynamic raw radio link characteristics and computes a composite EIGRP cost metric based on a proprietary formula. To avoid churn in the network as a result of the change in the link characteristics, a tunable dampening mechanism is used.

EIGRP uses the metric weights along with a set of vector metrics to compute the composite metric for local RIB installation and route selections. The EIGRP composite metric is calculated using the formula:

\[
\text{EIGRP Metric} = 256\times((K1\times Bw) + (K2\times Bw)/(256-Load) + (K3\times Delay)\times(K5/(\text{Reliability} + K4)))
\]

Table 1 lists the EIGRP vector metrics and their descriptions.

<table>
<thead>
<tr>
<th>Vector Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>Minimum bandwidth of the route in kilobits per second. It can be 0 or any positive integer. The bandwidth for the formula is scaled and inverted by the following formula: (10^7/\text{minimum Bw in kilobits per second})</td>
</tr>
<tr>
<td>delay</td>
<td>Route delay in tens of microseconds.</td>
</tr>
<tr>
<td>delay reliability</td>
<td>Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100 percent reliability; 0 means no reliability.</td>
</tr>
</tbody>
</table>
Configuring EIGRP

Information About EIGRP

EIGRP monitors metric weights on an interface to allow for the tuning of EIGRP metric calculations and indicate type of service (ToS). Table 2 lists the K values and their default.

Table 2  EIGRP K-Value Defaults

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>K1</td>
<td>1</td>
</tr>
<tr>
<td>K2</td>
<td>0</td>
</tr>
<tr>
<td>K3</td>
<td>1</td>
</tr>
<tr>
<td>K4</td>
<td>0</td>
</tr>
<tr>
<td>K5</td>
<td>0</td>
</tr>
</tbody>
</table>

Most configurations use the delay and bandwidth metrics, with bandwidth taking precedence. The default formula of $256 \times (Bw + Delay)$ is the EIGRP metric. The bandwidth for the formula is scaled and inverted by the following formula:

\[
\frac{10^7}{\text{minimum Bw in kilobits per second}}
\]

You can change the weights, but these weights must be the same on all the routers.

For example, look at a link whose bandwidth to a particular destination is 128k and the delay is 84,000 microseconds.

Using the cut-down formula, the EIGRP metric calculation would simplify to $256 \times (Bw + Delay)$, resulting in the following value:

\[
\text{Metric} = 256 \times (\frac{10^7}{128} + \frac{84000}{10}) = 256 \times 86525 = 22150400
\]

To calculate route delay, divide the delay value by 10 to get the true value in tenths of microseconds.

When EIGRP calculates the delay for Mobile Ad Hoc Networks (MANET) and the delay is obtained from a router interface, the delay is always calculated in tens of microseconds. In most cases, when using MANET, you will not use the interface delay, but rather the delay that is advertised by the radio. The delay you will receive from the radio is in microseconds, so you must adjust the cut-down formula as follows:

\[
\text{Metric} = (256 \times (\frac{10^7}{128}) + (84000 \times 256) / 10) = 20000000 + 2150400 = 22150400
\]
Route Summarization

You can configure EIGRP to perform automatic summarization of subnet routes into network-level routes. For example, you can configure subnet 172.16.1.0 to be advertised as 172.16.0.0 over interfaces that have subnets of 192.168.7.0 configured. Automatic summarization is performed when two or more network (EIGRP) router configuration or address family configuration commands are configured for the EIGRP process. By default, this feature is enabled.

Route summarization works in conjunction with the `ip summary-address eigrp` interface configuration command for autonomous system configurations and with the `summary-address` (EIGRP) command for named configurations in which additional summarization can be performed. If automatic summarization is in effect, there usually is no need to configure network level summaries using the `ip summary-address eigrp` command.

Summary Aggregate Addresses

You can configure a summary aggregate address for a specified interface. If any more specific routes are in the routing table, EIGRP will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes.

Floating Summary Routes

You can use a floating summary route when configuring the `ip summary-address eigrp` command for autonomous system configurations or the `summary-address` (EIGRP) command for named configurations. The floating summary route is created by applying a default route and administrative distance at the interface level, or address family interface level. The following scenarios illustrate the behavior of floating summary routes.

Figure 1 shows a network with three routers, Router-A, Router-B, and Router-C. Router-A learns a default route from elsewhere in the network and then advertises this route to Router-B. Router-B is configured so that only a default summary route is advertised to Router-C. The default summary route is applied to serial interface 0/1 on Router-B with the following configuration for an AS configuration:

```plaintext
Router(config)# interface Serial 0/1
Router(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0
```

The default summary route is applied to serial interface 0/1 on Router-B with the following configuration for a named configuration:

```plaintext
Router(config-router-af)# af-interface serial0/1
Router(config-router-af)# summary-address 192.168.0.0 255.255.0.0 95
```
The configuration of the default summary route on Router-B sends a 0.0.0.0/0 summary route to Router-C and blocks all other routes, including the 10.1.1.0/24 route, from being advertised to Router-C. However, this also generates a local discard route on Router-B, a route for 0.0.0.0/0 to the null 0 interface with an administrative distance of 5. When this route is created, it overrides the EIGRP learned default route. Router-B will no longer be able to reach destinations that it would normally reach through the 0.0.0.0.0/0 route.

This problem is resolved by applying a floating summary route to the interface on Router-B that connects to Router-C. The floating summary route is applied by configuring an administrative distance for the default summary route on the interface of Router-B with the following statement for an autonomous system configuration:

```
Router(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0 250
```

The floating summary route is applied by configuring an administrative distance for the default summary route on the interface of Router-B with the following statement for a named configuration:

```
Router(config-router-af-interface)# summary-address eigrp 100 0.0.0.0 0.0.0.0 250
```

The administrative distance of 250, applied in the above statement, is now assigned to the discard route generated on Router-B. The 0.0.0.0/0, from Router-A, is learned through EIGRP and installed in the local routing table. Routing to Router-C is restored.

If Router-A loses the connection to Router-B, Router-B will continue to advertise a default route to Router-C, which allows traffic to continue to reach destinations attached to Router-B. However, traffic destined to networks to Router-A or behind Router-A will be dropped when it reaches Router-B.

Figure 2 shows a network with two connections from the core, Router-A and Router-D. Both Router-B and Router-E have floating summary routes configured on the interfaces connected to Router-C. If the connection between Router-E and Router-C fails, the network will continue to operate normally. All traffic will flow from Router-C through Router-B to the hosts attached to Router-A and Router-D.
However, if the link between Router-A and Router-B fails, the network may incorrectly direct traffic because Router-B will continue to advertise the default route (0.0.0.0/0) to Router-C. In this scenario, Router-C still forwards traffic to Router-B, but Router-B drops the traffic. To avoid this problem, you should configure the summary address with an administrative distance on only single-homed remote routers or areas where there is only one exit point between two segments of the network. If two or more exit points exist (from one segment of the network to another), configuring the floating default route can cause a black hole to be formed.

**EIGRP Route Authentication**

EIGRP route authentication provides message digest algorithm 5 (MD5) authentication of routing updates from the EIGRP routing protocol. The MD5 keyed digest in each EIGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

Each key has its own key identifier (specified with the `key number` key chain configuration command), which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and MD5 authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters. Note that the router needs to know the time to configure keys with lifetimes. Refer to the Network Time Protocol (NTP) and calendar commands in the “Performing Basic System Management” module of the *Cisco IOS Network Management Configuration Guide*.
For AS and named configuration examples of route authentication, see the “EIGRP Route Authentication: Autonomous System Configuration Example” section on page 58 and the “EIGRP Route Authentication: Named Configuration Example” section on page 59.

Hello Packets and the Hold-Time Intervals

You can adjust the interval between hello packets and the hold time. This is a protocol-independent parameter that works for AppleTalk, IP, and IPX.

Routing devices periodically send hello packets to each other to dynamically learn of other routers on their directly attached networks. This information is used to discover neighbors and to learn when neighbors become unreachable or inoperative.

By default, hello packets are sent every 5 seconds. The exception is on low-speed, nonbroadcast multiaccess (NBMA) media, where the default hello interval is 60 seconds. Low speed is considered to be a rate of T1 or slower, as specified with the bandwidth interface configuration command. The default hello interval remains 5 seconds for high-speed NBMA networks. Note that for the purposes of EIGRP, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may or may not be considered to be NBMA. These networks are considered NBMA only if the interface has not been configured to use physical multicasting.

You can configure the hold time on a specified interface for a particular EIGRP routing process designated by the autonomous system number. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The default hold time is three times the hello interval, or 15 seconds. For slow-speed NBMA networks, the default hold time is 180 seconds.

On very congested and large networks, the default hold time might not be sufficient for all routers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

Note

Do not adjust the hold time without advising your technical support personnel.

Split Horizon

Split horizon controls the sending of EIGRP update and query packets. This is a protocol-independent parameter that works for IP and IPX. When split horizon is enabled on an interface, update and query packets are not sent for destinations for which this interface is the next hop. Controlling update and query packets in this manner reduces the possibility of routing loops.

By default, split horizon is enabled on all interfaces.

Split horizon blocks route information from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routing devices, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and SMDS), situations can arise for which this behavior is less than ideal. For these situations, including networks in which you have EIGRP configured, you may want to disable split horizon.

Link Bandwidth Percentage

By default, EIGRP packets consume a maximum of 50 percent of the link bandwidth, as configured with the bandwidth interface configuration command for AS configurations, and with the bandwidth-percent command for named configurations. You might want to change that value if a
different level of link utilization is required or if the configured bandwidth does not match the actual link bandwidth (it may have been configured to influence route metric calculations). This is a protocol-independent parameter that works for IP and IPX.

**EIGRP Stub Routing**

The EIGRP Stub Routing feature improves network stability, reduces resource utilization, and simplifies stub router configuration.

Stub routing is commonly used in a hub-and-spoke network topology. In a hub-and-spoke network, one or more end (stub) networks are connected to a remote router (the spoke) that is connected to one or more distribution routers (the hub). The remote router is adjacent only to one or more distribution routers. The only route for IP traffic to follow into the remote router is through a distribution router. This type of configuration is commonly used in WAN topologies where the distribution router is directly connected to a WAN. The distribution router can be connected to many more remote routers. Often, the distribution router will be connected to many remote routers. In a hub-and-spoke topology, the remote router must forward all nonlocal traffic to a distribution router, so it becomes unnecessary for the remote router to hold a complete routing table. Generally, the distribution router need not send anything more than a default route to the remote router.

When using the EIGRP Stub Routing feature, you need to configure the distribution and remote routers to use EIGRP, and to configure only the remote router as a stub. Only specified routes are propagated from the remote (stub) router. The stub router responds to all queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message “inaccessible.” A router that is configured as a stub will send a special peer information packet to all neighboring routers to report its status as a stub router.

Any neighbor that receives a packet informing it of the stub status will not query the stub router for any routes, and a router that has a stub peer will not query that peer. The stub router will depend on the distribution router to send the proper updates to all peers.

Figure 3 shows a simple hub-and-spoke configuration.

![Simple Hub-and-Spoke Network](image)

The stub routing feature by itself does not prevent routes from being advertised to the remote router. In the example in Figure 3, the remote router can access the corporate network and the Internet through the distribution router only. Having a full route table on the remote router, in this example, would serve no functional purpose because the path to the corporate network and the Internet would always be through the distribution router. The larger route table would only reduce the amount of memory required by the
remote router. Bandwidth and memory can be conserved by summarizing and filtering routes in the distribution router. The remote router need not receive routes that have been learned from other networks because the remote router must send all nonlocal traffic, regardless of destination, to the distribution router. If a true stub network is desired, the distribution router should be configured to send only a default route to the remote router. The EIGRP Stub Routing feature does not automatically enable summarization on the distribution router. In most cases, the network administrator will need to configure summarization on the distribution routers.

**Note**

When configuring the distribution router to send only a default route to the remote router, you must use the `ip classless` command on the remote router. By default, the `ip classless` command is enabled in all Cisco IOS images that support the EIGRP Stub Routing feature.

Without the stub feature, even after the routes that are sent from the distribution router to the remote router have been filtered or summarized, a problem might occur. If a route is lost somewhere in the corporate network, EIGRP could send a query to the distribution router, which in turn would send a query to the remote router even if routes are being summarized. If there is a problem communicating over the WAN link between the distribution router and the remote router, an EIGRP stuck in active (SIA) condition could occur and cause instability elsewhere in the network. The EIGRP Stub Routing feature allows a network administrator to prevent queries from being sent to the remote router.

### Dual-Homed Remote Topology

In addition to a simple hub-and-spoke network where a remote router is connected to a single distribution router, the remote router can be dual-homed to two or more distribution routers. This configuration adds redundancy and introduces unique issues, and the stub feature helps to address some of these issues.

A dual-homed remote router will have two or more distribution (hub) routers. However, the principles of stub routing are the same as they are with a hub-and-spoke topology. **Figure 4** shows a common dual-homed remote topology with one remote router, but 100 or more routers could be connected on the same interfaces on distribution router 1 and distribution router 2. The remote router will use the best route to reach its destination. If distribution router 1 experiences a failure, the remote router can still use distribution router 2 to reach the corporate network.

**Figure 4**  
*Simple Dual-Homed Remote Topology*
Figure 4 shows a simple dual-homed remote with one remote router and two distribution routers. Both distribution routers maintain routes to the corporate network and stub network 10.1.1.0/24.

Dual-homed routing can introduce instability into an EIGRP network. In Figure 5, distribution router 1 is directly connected to network 10.3.1.0/24. If summarization or filtering is applied on distribution router 1, the router will advertise network 10.3.1.0/24 to all of its directly connected EIGRP neighbors (distribution router 2 and the remote router).

Figure 5 shows a simple dual-homed remote router where distribution router 1 is connected to both network 10.3.1.0/24 and network 10.2.1.0/24.

If the 10.2.1.0/24 link between distribution router 1 and distribution router 2 has failed, the lowest cost path to network 10.3.1.0/24 from distribution router 2 is through the remote router (see Figure 6). This route is not desirable because the traffic that was previously traveling across the corporate network 10.2.1.0/24 would now be sent across a much lower bandwidth connection. The over utilization of the lower bandwidth WAN connection can cause a number of problems that might affect the entire corporate network. The use of the lower bandwidth route that passes through the remote router might cause WAN EIGRP distribution routers to be dropped. Serial lines on distribution and remote routers could also be dropped, and EIGRP SIA errors on the distribution and core routers could occur.
It is not desirable for traffic from distribution router 2 to travel through any remote router in order to reach network 10.3.1.0/24. If the links are sized to handle the load, it would be acceptable to use one of the backup routes. However, most networks of this type have remote routers located at remote offices with relatively slow links. This problem can be prevented if proper summarization is configured on the distribution router and remote router.

It is typically undesirable for traffic from a distribution router to use a remote router as a transit path. A typical connection from a distribution router to a remote router would have much less bandwidth than a connection at the network core. Attempting to use a remote router with a limited bandwidth connection as a transit path would generally produce excessive congestion to the remote router. The EIGRP Stub Routing feature can prevent this problem by preventing the remote router from advertising core routes back to distribution routers. Routes learned by the remote router from distribution router 1 will not be advertised to distribution router 2. Because the remote router will not advertise core routes to distribution router 2, the distribution router will not use the remote router as a transit for traffic destined for the network core.

The EIGRP Stub Routing feature can help to provide greater network stability. In the event of network instability, this feature prevents EIGRP queries from being sent over limited bandwidth links to nontransit routers. Instead, distribution routers to which the stub router is connected answer the query on behalf of the stub router. This feature greatly reduces the chance of further network instability due to congested or problematic WAN links. The EIGRP Stub Routing feature also simplifies the configuration and maintenance of hub-and-spoke networks. When stub routing is enabled in dual-homed remote configurations, it is no longer necessary to configure filtering on remote routers to prevent those remote routers from appearing as transit paths to the hub routers.

**Caution**

The EIGRP Stub Routing feature should be used only on stub routers. A stub router is defined as a router connected to the network core or distribution layer through which core transit traffic should not flow. A stub router should not have any EIGRP neighbors other than distribution routers. Ignoring this restriction will cause undesirable behavior.
Multi access interfaces such as ATM, Ethernet, Frame Relay, ISDN PRI, and X.25 are supported by the EIGRP Stub Routing feature only when all routers on that interface, except the hub, are configured as stub routers.

### EIGRP Stub Routing Leak Map Support

In EIGRP stub routing configurations where there is a remote site with more than one router, only one of the remote routers can be configured as the stub router. If you have two distribution layer routers, and two routers at a remote site, there is no way to declare both remote routers as stub routers. If one remote router is configured as a stub router, the other remote router cannot learn routes toward the network core if the link between the stub router and the distribution layer router fails and cannot route around the failed link.

The stub router cannot readvertise routes it has learned from any neighboring EIGRP router. To resolve this, a leak map configuration can be added to the EIGRP stub routing feature that allows a selected set of learned routes to be readvertised to other peers. The set of routes allowed through the stub router are specified using a standard route map, so that routes can be matched based on tags, prefixes, or interfaces. These routes are marked using the site of origin code mechanism, which prevents the routes permitted through the stub from being readvertised into the core of the network.

Configure the `eigrp stub` command with the `leak-map` keyword to configure the EIGRP stub routing feature to reference a leak map that identifies routes that are allowed to be advertised on an EIGRP stub router that would normally have been suppressed.

### How to Configure EIGRP

- Enabling EIGRP: Autonomous System Configuration, page 17 (required)
- Enabling EIGRP: Named Configuration, page 18 (required)
- Configuring Optional EIGRP Parameters: Autonomous System Configuration, page 19 (optional)
- Configuring Optional EIGRP Parameters: Named Configuration, page 21 (optional)
- Configuring EIGRP Redistribution: Autonomous System Configuration, page 23 (optional)
- Configuring EIGRP Redistribution: Named Configuration, page 25 (optional)
- Configuring EIGRP Route Summarization: Autonomous System Configuration, page 27 (optional)
- Configuring EIGRP Route Summarization: Named Configuration, page 28 (optional)
- Configuring EIGRP Event Logging: Autonomous System Configuration, page 30 (optional)
- Configuring EIGRP Event Logging: Named Configuration, page 31 (optional)
- Configuring Equal and Unequal Cost Load Balancing: Autonomous System Configuration, page 33 (optional)
- Configuring Equal and Unequal Cost Load Balancing: Named Configuration, page 34 (optional)
- Configuring EIGRP Route Authentication: Autonomous System Configuration, page 35 (optional)
- Configuring EIGRP Route Authentication: Named Configuration, page 37 (optional)
- Adjusting the Interval Between Hello Packets and the Hold Time: Autonomous System Configuration, page 39 (optional)
- Adjusting the Interval Between Hello Packets and the Hold Time: Named Configuration, page 41 (optional)
- Disabling Split Horizon: Autonomous System Configuration, page 43 (optional)
- Disabling Split Horizon and Next-Hop-Self: Named Configuration, page 43 (optional)
- Configuring EIGRP Stub Routing: Autonomous System Configuration, page 45 (optional)
- Configuring EIGRP Stub Routing: Named Configuration, page 46 (optional)
- Monitoring and Maintaining EIGRP: Autonomous System Configuration, page 48 (optional)
- Monitoring and Maintaining EIGRP: Named Configuration, page 50 (optional)

**Enabling EIGRP: Autonomous System Configuration**

Perform this task to enable EIGRP and create an EIGRP routing process. EIGRP sends updates to the interfaces in the specified networks. If you do not specify the network of an interface, the interface will not be advertised in any EIGRP update.

Configuring the `router eigrp` command with the `autonomous-system-number` argument creates an EIGRP configuration referred to as an autonomous system configuration. EIGRP AS configuration creates an EIGRP routing instance that can be used for tagging routing information.

**SUMMARY STEPS**

1. `enable`  
2. `configure terminal`  
3. `router eigrp autonomous-system-number`  
4. `network network-number`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** router eigrp autonomous-system-number | Configures an EIGRP routing process and enters router configuration mode.  
- A maximum of 30 EIGRP routing processes can be configured. |
| **Example:** Router(config)# router eigrp 1 | |
| **Step 4** network network-number | Associates networks with an EIGRP routing process. |
| **Example:** Router(config-router)# network 172.16.0.0 | |
Enabling EIGRP: Named Configuration

Perform this task to enable EIGRP and to create an EIGRP routing process. EIGRP sends updates to the interfaces in the specified networks. If you do not specify the network of an interface, the interface will not be advertised in any EIGRP update.

Configuring the `router eigrp` command with the `virtual-instance-name` argument creates an EIGRP configuration referred to as EIGRP named configuration. EIGRP named configuration does not create an EIGRP routing instance by itself. EIGRP named configuration is a base configuration that is required to define address family configurations under it that are used for routing.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router eigrp virtual-instance-name`
4. `address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
   or
   `address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
5. `network ip-address [wildcard-mask]`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router eigrp virtual-instance-name</td>
<td>Configures the EIGRP routing process.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# router eigrp virtual-name1</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Optional EIGRP Parameters: Autonomous System Configuration

Perform this task to configure optional EIGRP parameters including applying offsets to routing metrics, adjusting EIGRP metrics, and disabling automatic summarization in an EIGRP AS configuration.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `router eigrp autonomous-system`
4. `network ip-address [wildcard-mask]`
5. `passive-interface [default] [interface-type interface-number]`
6. `offset-list [access-list-number | access-list-name] [in | out] offset [interface-type interface-number]`
7. `metric weights tos k1 k2 k3 k4 k5`
8. `no auto-summary`
9. `exit`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.</td>
</tr>
<tr>
<td><code>address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</code></td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><code>address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-router)# address-family ipv4 autonomous-system 45000</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Specifies a network for the EIGRP routing process.</td>
</tr>
<tr>
<td><code>network ip-address [wildcard-mask]</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-router-af)# network 172.16.0.0</code></td>
<td></td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> en<strong>able</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router eigrp autonomous-system</td>
<td>Enables an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# router eigrp 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> network ip-address [wildcard-mask]</td>
<td>Associates networks with an EIGRP routing process.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router)# network 172.16.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> passive-interface [default] [interface-type interface-number]</td>
<td>(Optional) Suppresses EIGRP hello packets and routing updates on interfaces while still including the interface addresses in the topology database.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router)# passive-interface</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> offset-list [access-list-number</td>
<td>(Optional) Applies an offset to routing metrics.</td>
</tr>
<tr>
<td>access-list-name] in</td>
<td>out] offset [interface-type interface-number]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router)# offset-list 21 in 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> metric weights tos k1 k2 k3 k4 k5</td>
<td>(Optional) Adjusts the EIGRP metric or K value.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router)# metric weights 0 2 0 2 0 0</td>
<td></td>
</tr>
</tbody>
</table>

**Note** If K5 is 0 then (K5/(Reliability + K4)) is defined as 1.
### Configuring Optional EIGRP Parameters: Named Configuration

Perform this task to configure optional EIGRP named configuration parameters including applying offsets to routing metrics, adjusting EIGRP metrics, and disabling automatic summarization.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `router eigrp virtual-instance-name`
4. `address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
   or

   `address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
5. `network ip-address [wildcard-mask]`
6. `metric weights tos k1 k2 k3 k4 k5`
7. `af-interface {default | interface-type interface-number}`
8. `passive-interface [default] [interface-type interface-number]`
9. `bandwidth-percent maximum-bandwidth-percentage`
10. `exit-af-interface`
11. `topology { base | topology-name tid number }`
12. `offset-list [access-list-number | access-list-name] { in | out } offset [interface-type interface-number]`
13. `no auto-summary`
14. `exit-af-topology`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8 no auto-summary</td>
<td>(Optional) Disables automatic summarization. Note: Automatic summarization is enabled by default.</td>
</tr>
<tr>
<td>Example: Router(config-router)# no auto-summary</td>
<td></td>
</tr>
<tr>
<td>Step 9 exit</td>
<td>Exits router configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-router)# exit</td>
<td></td>
</tr>
</tbody>
</table>

#### Example:

Command or Action | Purpose |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no auto-summary</code></td>
<td>(Optional) Disables automatic summarization. Note: Automatic summarization is enabled by default.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits router configuration mode.</td>
</tr>
</tbody>
</table>
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** router eigrp virtual-instance-name | Enables an EIGRP routing process and enters router configuration mode. |
| **Example:** Router(config)# router eigrp virtual-name1 | |
| **Step 4** address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number | Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance. |
| or address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number | |
| **Example:** Router(config-router)# address-family ipv4 autonomous-system 45000 | |
| **Step 5** network ip-address [ wildcard-mask] | Specifies a network for the EIGRP routing process. |
| **Example:** Router(config-router-af)# network 172.16.0.0 | |
| **Step 6** metric weights tos k1 k2 k3 k4 k5 | (Optional) Adjusts the EIGRP metric or K value.  
  - EIGRP uses the following formula to determine the total metric to the network:  
    \[
    \text{EIGRP Metric} = 256 \ast ((K1 \ast Bw) + (K2 \ast Bw)/(256 - \text{Load}) + (K3 \ast \text{Delay}) \ast (K5/(\text{Reliability} + K4)))
    \]  
  **Note** If K5 is 0 then \((K5/(\text{Reliability} + K4))\) is defined as 1. |
| **Example:** Router(config-router-af)# metric weights 0 2 0 2 0 0 | |
| **Step 7** af-interface {default | interface-type interface-number} | Enters address family interface configuration mode and configures interface-specific EIGRP commands. |
| **Example:** Router(config-router-af)# af-interface ethernet0/0 | |
Configuring EIGRP Redistribution: Autonomous System Configuration

Perform this task to configure redistribution of non-EIGRP protocol metrics into EIGRP metrics and to configure the EIGRP administrative distance in an EIGRP AS configuration.

You must use a default metric to redistribute a protocol into EIGRP, unless you use the `redistribute` command.

Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td><code>passive-interface [default] [interface-type interface-number]</code></td>
<td>Suppresses EIGRP hello packets and routing updates on interfaces while still including the interface addresses in the topology database.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-router-af-interface)# passive-interface</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>bandwidth-percent maximum-bandwidth-percentage</code></td>
<td>Configures the percentage of bandwidth that may be used by an EIGRP address family on an interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-router-af-interface)# bandwidth-percent 75</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>exit-af-interface</code></td>
<td>Exits address family interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-router-af-interface)# exit-af-interface</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>`topology {base</td>
<td>topology-name tid number}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-router-af)# topology base</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>`offset-list [access-list-number</td>
<td>access-list-name] {in</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-router-af-topology)# offset-list 21 in 10 ethernet 0</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td><code>no auto-summary</code></td>
<td>(Optional) Disables automatic summarization. <strong>Note</strong> Automatic summarization is enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-router-af-topology)# no auto-summary</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><code>exit-af-topology</code></td>
<td>Exits address family topology configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-router-af-topology)# exit-af-topology</td>
<td></td>
</tr>
</tbody>
</table>
Default metrics are supported only when you are redistributing from EIGRP or static routes.

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `router eigrp autonomous-system`
4. `network ip-address [wildcard-mask]`
5. `redistribute protocol [process-id] (level-1 | level-1-2 | level-2) [autonomous-system-number] [metric {metric-value | transparent}] [metric-type type-value] [match {internal | external 1 | external 2}] [tag tag-value] [route-map map-tag] [subnets]`
6. `distance eigrp internal-distance external-distance`
7. `default-metric bandwidth delay reliability loading mtu`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| `enable`          | Enables privileged EXEC mode. |
| Example:
| Router> enable    | • Enter your password if prompted. |
| **Step 2**
| `configure terminal` | Enters global configuration mode. |
| Example:
| Router# configure terminal |
| **Step 3**
| `router eigrp autonomous-system` | Enables an EIGRP routing process and enters router configuration mode. |
| Example:
| Router(config)# router eigrp 1 | • A maximum of 30 EIGRP routing processes can be configured. |
| **Step 4**
| Example:
| Router(config-router)# network 172.16.0.0 |
| **Step 5**
| `redistribute protocol [process-id] (level-1 | level-1-2 | level-2) [autonomous-system-number] [metric {metric-value | transparent}] [metric-type type-value] [match {internal | external 1 | external 2}] [tag tag-value] [route-map map-tag] [subnets]` | Redistributes routes from one routing domain into another routing domain. |
| Example:
| Router(config-router)# redistribute rip |
Configuring EIGRP

How to Configure EIGRP

Configuring EIGRP Redistribution: Named Configuration

Perform this task to configure redistribution of non-EIGRP protocol metrics into EIGRP metrics and to configure EIGRP administrative distance in an EIGRP named configuration.

You must use a default metric to redistribute a protocol into EIGRP, unless you use the `redistribute` command.

Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values.

Default metrics are supported only when you are redistributing from EIGRP or static routes.

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

SUMMARY STEPS

1. enable
2. configure terminal
3. router eigrp virtual-instance-name
4. address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number
   or
   address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number
5. af-interface {default | interface-type interface-number}
6. no shutdown
7. exit-af-interface
8. topology { base | topology-name tid number}
9. distance eigrp internal-distance external-distance
10. redistribute eigrp virtual-instance-name [autonomous-system-number]

Step 6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>distance eigrp internal-distance external-distance</td>
<td>Allows the use of two administrative distances—internal and external—that could be a better route to a node.</td>
</tr>
</tbody>
</table>

Example:

Router(config-router)# distance eigrp 80 130

Step 7

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-metric bandwidth delay reliability loading mtu</td>
<td>Sets metrics for EIGRP.</td>
</tr>
</tbody>
</table>

Example:

Router(config-router)# default-metric 1000 100 250 100 1500

Example: (continues)

Router(config-router)# distance eigrp 80 130

Sets metrics for EIGRP.

Example: (continues)

Router(config-router)# default-metric 1000 100 250 100 1500
11. **default-metric** *bandwidth delay reliability loading mtu*

12. **exit-af-topology**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
| Example: Router> enable | • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Router# configure terminal | |
| **Step 3** router eigrp virtual-instance-name | Enables an EIGRP routing process and enters router configuration mode. |
| Example: Router(config)# router eigrp virtual-name1 | |
| **Step 4** address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number  

or  

address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number | Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance. |
| Example: Router(config-router)# address-family ipv4 autonomous-system 45000 | |
| **Step 5** af-interface {default | interface-type interface-number} | Enters address family interface configuration mode and configures interface-specific EIGRP commands. |
| Example: Router(config-router-af)# af-interface ethernet0/0 | |
| **Step 6** no shutdown | Restarts a disabled interface. |
| Example: Router(config-router-af)# no shutdown | |
| **Step 7** exit-af-interface | Exits address family interface configuration mode. |
| Example: Router(config-router-af-interface)# exit-af-interface | |
Configuring EIGRP Route Summarization: Autonomous System Configuration

Perform this task to configure EIGRP to perform automatic summarization of subnet routes into network-level routes in an EIGRP AS configuration.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. router eigrp autonomous-system
4. exit
5. interface type/number
6. ip summary-address eigrp as-number ip-address mask [admin-distance] [leak-map name]
7. ip bandwidth-percent eigrp as-number percent
DETAILED STEPS

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  
**router eigrp autonomous-system**  

Example:  
Router(config)# router eigrp 101  
Enables an EIGRP routing process and enters router configuration mode.  
• A maximum of 30 EIGRP routing processes can be configured.

Step 4  
**exit**  

Example:  
Router(config-router)# exit  
Exits router configuration mode.

Step 5  
**interface type/number**  

Example:  
Router(config)# interface ethernet0/0  
Enters interface configuration mode.

Step 6  
**ip summary-address eigrp as-number ip-address mask [admin-distance] [leak-map name]**  

Example:  
Router(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0  
(Optional) Configures a summary aggregate address.

Step 7  
**ip bandwidth-percent eigrp as-number percent**  

Example:  
Router(config-if)# ip bandwidth-percent eigrp 209 75  
(Optional) Configures the percentage of bandwidth that may be used by EIGRP on an interface.

Configuring EIGRP Route Summarization: Named Configuration

Perform this task to configure EIGRP to perform automatic summarization of subnet routes into network-level routes in an EIGRP named configuration.

SUMMARY STEPS

1.  
**enable**

2.  
**configure terminal**

3.  
**router eigrp virtual-instance-name**
4. address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number
   or
   address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number

5. af-interface {default | interface-type interface-number}

6. summary-address ip-address mask [administrative-distance [leak-map leak-map-name]]

7. exit-af-interface

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>router eigrp virtual-instance-name</td>
<td>Enables an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# router eigrp virtual-name1</td>
</tr>
<tr>
<td>Step 4 address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
<td>Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.</td>
</tr>
<tr>
<td>or</td>
<td>Router(config-router)# address-family ipv4 autonomous-system 45000</td>
</tr>
<tr>
<td>af-interface {default</td>
<td>interface-type interface-number}</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router-af)# af-interface ethernet0/0</td>
</tr>
</tbody>
</table>
Configuring EIGRP

How to Configure EIGRP

Perform the following task to configure EIGRP event logging parameters for an EIGRP AS configuration.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. router eigrp autonomous-system
4. eigrp event-log-size size
5. eigrp log-neighbor-changes
6. eigrp log-neighbor-warnings [seconds]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 router eigrp autonomous-system</td>
<td>Enables an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>A maximum of 30 EIGRP routing processes can be configured.</td>
</tr>
</tbody>
</table>

---

**Configuring EIGRP Event Logging: Autonomous System Configuration**

Perform the following task to configure EIGRP event logging parameters for an EIGRP AS configuration.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. router eigrp autonomous-system
4. eigrp event-log-size size
5. eigrp log-neighbor-changes
6. eigrp log-neighbor-warnings [seconds]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6 summary-address ip-address mask [administrative-distance [leak-map leak-map-name]]</td>
<td>Configures a summary address for EIGRP.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router-af-interface)# summary-address 192.168.0.0 255.255.0.0</td>
</tr>
<tr>
<td>Step 7 exit-af-interface</td>
<td>Exits address family interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router-af-interface)# exit-af-interface</td>
</tr>
</tbody>
</table>

---

**Example:**

Router(config-router-af-interface)# summary-address 192.168.0.0 255.255.0.0

Configures a summary address for EIGRP.

Router(config-router-af-interface)# exit-af-interface

Exits address family interface configuration mode.
Configuring EIGRP Event Logging: Named Configuration

Perform the following task to configure EIGRP event logging parameters for an EIGRP named configuration.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router eigrp virtual-instance-name**
4. **address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number**
   or
   **address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number**
5. **eigrp log-neighbor-warnings [seconds]**
6. **eigrp log-neighbor-changes**
7. **topology {base | topology-name tid number}**
8. **eigrp event-log-size size**

---

**Step 4**

```plaintext
Step 4 eigrp event-log-size size
```

(Optional) Sets the size of the EIGRP event log.

**Example:**

```
Router(config-router)# eigrp event-log-size 5000010
```

**Step 5**

```plaintext
Step 5 eigrp log-neighbor-changes
```

(Optional) Enables logging of EIGRP neighbor adjacency changes.

- By default, the system logs EIGRP neighbor adjacency changes to help you monitor the stability of the routing system and detect problems.

**Example:**

```
Router(config-router)# eigrp log-neighbor-changes
```

**Step 6**

```plaintext
Step 6 eigrp log-neighbor-warnings [seconds]
```

(Optional) Enables the logging of EIGRP neighbor warning messages.

**Example:**

```
Router(config-router)# eigrp log-neighbor-warnings 300
```
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router eigrp virtual-instance-name</td>
<td>Enables an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# router eigrp virtual-name1</td>
</tr>
<tr>
<td><strong>Step 4</strong> address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number or address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
<td>Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router)# address-family ipv4 autonomous-system 45000</td>
</tr>
<tr>
<td><strong>Step 5</strong> eigrp log-neighbor-warnings [seconds]</td>
<td>(Optional) Enables the logging of EIGRP neighbor warning messages.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router-af)# eigrp log-neighbor-warnings 300</td>
</tr>
<tr>
<td><strong>Step 6</strong> eigrp log-neighbor-changes</td>
<td>(Optional) Enables logging of EIGRP neighbor adjacency changes.</td>
</tr>
<tr>
<td>Example:</td>
<td>By default, the system logs EIGRP neighbor adjacency changes to help you monitor the stability of the routing system and detect problems.</td>
</tr>
<tr>
<td><strong>Step 7</strong> topology base</td>
<td>Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router-af)# topology base</td>
</tr>
<tr>
<td><strong>Step 8</strong> eigrp event-log-size size</td>
<td>(Optional) Sets the size of the EIGRP event log.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router-af-topology)# eigrp event-log-size 10000</td>
</tr>
</tbody>
</table>
**Configuring Equal and Unequal Cost Load Balancing: Autonomous System Configuration**

Perform the following task to configure EIGRP equal and unequal cost load balancing for an EIGRP AS configuration.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router eigrp autonomous-system**
4. **traffic-share balanced**
5. **maximum-paths number-of-paths**
6. **variance multiplier**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>router eigrp autonomous-system</strong></td>
<td>Enables an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# router eigrp 101</td>
<td>A maximum of 30 EIGRP routing processes can be configured.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>traffic-share balanced</strong></td>
<td>Controls how traffic is distributed among routes when multiple routes for the same destination network have different costs.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-router)# traffic-share balanced</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>maximum-paths number-of-paths</strong></td>
<td>Controls the maximum number of parallel routes that an IP routing protocol can support.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-router)# maximum-paths 5</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>variance multiplier</strong></td>
<td>Controls load balancing in an internetwork based on EIGRP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-router)# variance 1</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Equal and Unequal Cost Load Balancing: Named Configuration

Perform the following task to configure EIGRP equal and unequal cost load balancing for an EIGRP named configuration.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router eigrp virtual-instance-name`
4. `address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
   
   or
   
   `address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
5. `topology { base | topology-name tid number }
6. `traffic-share balanced`
7. `maximum-paths number-of-paths`
8. `variance multiplier`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>router eigrp virtual-instance-name</code></td>
<td>Enables an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config)# router eigrp virtual-name1</code></td>
<td></td>
</tr>
</tbody>
</table>
| **Step 4** `address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
   
   or
   
   `address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
| **Example:** `Router(config-router)# address-family ipv4 autonomous-system 45000` | Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance. |
### Configuring EIGRP Route Authentication: Autonomous System Configuration

Before you can configure EIGRP route authentication, you must enable EIGRP. Perform the following task to configure authentication of EIGRP packets in an EIGRP autonomous system configuration.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot`
4. `ip authentication mode eigrp autonomous-system md5`
5. `ip authentication key-chain eigrp autonomous-system key-chain`
6. `exit`
7. `key chain name-of-chain`
8. `key key-id`
9. `key-string text`
10. `accept-lifetime start-time {infinite | end-time | duration seconds}`
11. `send-lifetime start-time {infinite | end-time | duration seconds}`

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>`topology {base</td>
<td>topology-name tid number}`</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-router-af)# topology base</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>traffic-share balanced</code></td>
<td>Controls how traffic is distributed among routes when multiple routes for the same destination network have different costs.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-router-af-topology)# traffic-share balanced</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>maximum-paths number-of-paths</code></td>
<td>Controls the maximum number of parallel routes that an IP routing protocol can support.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-router-af-topology)# maximum-paths 5</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>variance multiplier</code></td>
<td>Controls load balancing in an internetwork based on EIGRP.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-router-af-topology)# variance 1</td>
<td></td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot</td>
<td>Configures an interface type and enters interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface Ethernet0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip authentication mode eigrp autonomous-system md5</td>
<td>Enables MD5 authentication in EIGRP packets.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-if) ip authentication mode eigrp 1 md5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip authentication key-chain eigrp autonomous-system key-chain</td>
<td>Enables authentication of EIGRP packets.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip authentication key-chain eigrp 1 keychain1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> key chain name-of-chain</td>
<td>Identifies a key chain and enters keychain configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config)# key chain keychain1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> key key-id</td>
<td>Identifies the key number and enters key chain keyconfiguration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-keychain)# key 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> key-string text</td>
<td>Identifies the key string.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config-keychain-key)# key-string 0987654321</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring EIGRP Route Authentication: Named Configuration

Before you can configure EIGRP route authentication, you must enable EIGRP.

Perform the following task to configure authentication of EIGRP packets in an EIGRP named configuration.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `router eigrp virtual-instance-name`
4. `address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
   or
   `address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
5. `network ip-address [wildcard-mask]`
6. `af-interface {default | interface-type interface-number}`
7. `authentication key-chain name-of-chain`
8. `authentication mode md5`
9. `exit-af-interface`
10. `exit-address-family`
11. `exit`
12. `key chain name-of-chain`
13. `key key-id`
14. `key-string text`
15. `accept-lifetime start-time {infinite | end-time | duration seconds}`
16. `send-lifetime start-time {infinite | end-time | duration seconds}`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`accept-lifetime start-time {infinite</td>
<td>end-time</td>
</tr>
<tr>
<td>`send-lifetime start-time {infinite</td>
<td>end-time</td>
</tr>
</tbody>
</table>

**Example:**

Router(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite

Step 11

Example:

Router(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
## How to Configure EIGRP

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router eigrp virtual-instance-name</td>
<td>Enables an EIGRP routing process and enters router configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# router eigrp virtual-name1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number or address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
<td>Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router)# address-family ipv4 autonomous-system 45000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> network ip-address [wildcard-mask]</td>
<td>Associates networks with an EIGRP routing process.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af)# network 172.16.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> af-interface {default</td>
<td>interface-type interface-number}</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af)# af-interface ethernet0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> authentication key-chain name-of-chain</td>
<td>Specifies an authentication key chain for EIGRP.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af-interface)# authentication key-chain SITE1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> authentication mode md5</td>
<td>Specifies the type of authentication used in an EIGRP address family for the EIGRP instance.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af-interface)# authentication mode md5</td>
<td></td>
</tr>
</tbody>
</table>
**Configuring EIGRP**

### Adjusting the Interval Between Hello Packets and the Hold Time: Autonomous System Configuration

Perform this task to adjust the interval between hello packets and the hold time in an EIGRP AS configuration.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>exit-af-interface</strong></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>exit-address-family</strong></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>key chain name-of-chain</strong></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>key key-id</strong></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>key-string text</strong></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>**accept-lifetime start-time {infinite</td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td>**send-lifetime start-time {infinite</td>
</tr>
</tbody>
</table>

**Example:**

- **Step 9**: `exit-af-interface`
  - Example: `Router(config-router-af-interface)# exit-af-interface`
  - Exits address family interface configuration mode.
- **Step 10**: `exit-address-family`
  - Example: `Router(config-router-af)# exit-address-family`
  - Exits address family configuration mode.
- **Step 11**: `exit`
  - Example: `Router(config-router)# exit`
  - Exits to global configuration mode.
- **Step 12**: `key chain name-of-chain`
  - Example: `Router(config)# key chain keychain1`
  - Identifies a key chain and enters keychain configuration mode.
- **Step 13**: `key key-id`
  - Example: `Router(config-keychain)# key 1`
  - Identifies the key number and enters keychain key configuration mode.
- **Step 14**: `key-string text`
  - Example: `Router(config-keychain-key)# key-string 0987654321`
  - Identifies the key string.
- **Step 15**: `accept-lifetime start-time {infinite | end-time | duration seconds}`
  - Example: `Router(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite`
  - (Optional) Specifies the time period during which the key can be received.
- **Step 16**: `send-lifetime start-time {infinite | end-time | duration seconds}`
  - Example: `Router(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite`
  - (Optional) Specifies the time period during which the key can be sent.
How to Configure EIGRP

Note
Do not adjust the hold time without advising your technical support personnel.

SUMMARY STEPS

1. enable
2. configure terminal
3. router eigrp autonomous-system-number
4. exit
5. interface slot/port
6. ip hello-interval eigrp autonomous-system-number seconds
7. ip hold-time eigrp autonomous-system-number seconds

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router eigrp autonomous-system-number</td>
<td>Enables an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# router eigrp 101</td>
<td>• A maximum of 30 EIGRP routing processes can be configured.</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits to global configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-router)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface slot/port</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# interface Ethernet0/1</td>
<td></td>
</tr>
</tbody>
</table>
Adjusting the Interval Between Hello Packets and the Hold Time: Named Configuration

Perform this task to adjust the interval between hello packets and the hold time in an EIGRP named configuration.

**Note** Do not adjust the hold time without advising your technical support personnel.

### SUMMARY STEPS

1. enable
2. configure terminal
3. router eigrp virtual-instance-name
4. address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number
   or
   address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number
5. af-interface {default | interface-type interface-number}
6. hello-interval seconds
7. hold-time seconds

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6 ip hello-interval eigrp autonomous-system-number seconds</td>
<td>Configures the hello interval for an EIGRP routing process.</td>
</tr>
<tr>
<td>Example: Router(config-if)# ip hello-interval eigrp 109 10</td>
<td></td>
</tr>
<tr>
<td>Step 7 ip hold-time eigrp autonomous-system-number seconds</td>
<td>Configures the hold time for an EIGRP routing process.</td>
</tr>
<tr>
<td>Example: Router(config-if)# ip hold-time eigrp 109 40</td>
<td>Note: Do not adjust the hold time without advising your technical support personnel.</td>
</tr>
</tbody>
</table>
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>router eigrp virtual-instance-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# router eigrp virtual-name1</td>
</tr>
<tr>
<td></td>
<td>Enables an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-router)# address-family ipv4 autonomous-system 45000</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-router)# address-family ipv6 autonomous-system 45000</td>
</tr>
<tr>
<td></td>
<td>Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>af-interface {default</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-router-af)# af-interface ethernet0/0</td>
</tr>
<tr>
<td></td>
<td>Enters address family interface configuration mode and configures interface-specific EIGRP commands.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>hello-interval seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-router-af-interface)# hello-interval 10</td>
</tr>
<tr>
<td></td>
<td>Configures the hello interval for an EIGRP address family named configuration.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>hold-time seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-router-af-interface)# hold-time 50</td>
</tr>
<tr>
<td></td>
<td>Configures the hold time for an EIGRP address family named configuration.</td>
</tr>
</tbody>
</table>
Disabling Split Horizon: Autonomous System Configuration

Split horizon controls the sending of EIGRP update and query packets. When split horizon is enabled on an interface, update and query packets are not sent for destinations for which this interface is the next hop. Controlling update and query packets in this manner reduces the possibility of routing loops.

By default, split horizon is enabled on all interfaces.

Perform the following task to disable split horizon for an EIGRP AS configuration.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface slot/port
4. no ip split-horizon eigrp autonomous-system-number

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Example:           |         |
| Router> enable     |         |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example:           |         |
| Router# configure terminal |         |
| **Step 3** interface slot/port | Enters interface configuration mode. |
| Example:           |         |
| Router(config)# interface Ethernet0/1 |         |
| **Step 4** no ip split-horizon eigrp autonomous-system-number | Disables split horizon. |
| Example:           |         |
| Router(config-if)# no ip split-horizon eigrp 101 |         |

Disabling Split Horizon and Next-Hop-Self: Named Configuration

Perform this task to disable EIGRP split horizon and next-hop-self for an EIGRP named configuration.

By default, split horizon is enabled on all interfaces.

EIGRP will, by default, set the next-hop value to the local outbound interface address for routes that it is advertising, even when advertising those routes back out the same interface where it learned them.

Perform this task to change this default to instruct EIGRP to use the received next hop value when advertising these routes. Disabling next-hop-self is primarily useful in Dynamic Multipoint VPN (DMVPN) spoke-to-spoke topologies.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router eigrp virtual-instance-name`
4. `address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
   or
   `address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
5. `af-interface {default | interface-type interface-number}`
6. `no split-horizon`
7. `no next-hop-self eigrp`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** router eigrp virtual-instance-name | Enables an EIGRP routing process and enters router configuration mode. |
| **Example:** Router(config)# router eigrp virtual-name1 | |
| **Step 4** address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number | Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance. |
| or | |
| **Example:** Router(config-router)# address-family ipv4 autonomous-system 45000 | |
| **Step 5** af-interface {default | interface-type interface-number} | Enters address family interface configuration mode and configures interface-specific EIGRP commands. |
| **Example:** Router(config-router-af)# af-interface ethernet0/0 | |
Configuring EIGRP Stub Routing: Autonomous System Configuration

Perform the following task to configure EIGRP stub routing for an EIGRP AS configuration.

SUMMARY STEPS

1. enable
2. configure terminal
3. router eigrp autonomous-system-number
4. network ip-address [wildcard-mask]
5. eigrp stub [receive-only] [leak-map name] [connected] [static] [summary] [redistributed]
6. exit
7. exit
8. show ip eigrp neighbors [interface-type | as-number | static | detail]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router eigrp autonomous-system-number</td>
<td>Configures a remote or distribution router to run an EIGRP process.</td>
</tr>
<tr>
<td>Example: Router(config)# router eigrp 1</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

#### Step 4
**network ip-address [wildcard-mask]**

**Example:**
Router(config-router)# network 172.16.0.0

**Purpose:** Specifies the network address of the EIGRP distribution router.

#### Step 5
**eigrp stub [receive-only] [leak-map name] [connected] [static] [summary] [redistributed]**

**Example:**
Router(config-router)# eigrp stub connected static

**Purpose:** Configures a remote router as an EIGRP stub router.

#### Step 6
**exit**

**Example:**
Router(config-router)# exit

**Purpose:** Exits router configuration mode.

#### Step 7
**exit**

**Example:**
Router(config)# exit

**Purpose:** Exits global configuration mode.

#### Step 8
**show ip eigrp neighbors [interface-type | as-number | static | detail]**

**Example:**
Router# show ip eigrp neighbors detail

**Purpose:** (Optional) Verifies that a remote router has been configured as a stub router with EIGRP. Enter this command from the distribution router. The last line of the output displays the stub status of the remote or spoke router.

### Configuring EIGRP Stub Routing: Named Configuration

Perform the following task to configure EIGRP stub routing for an EIGRP named configuration.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp virtual-instance-name**
4. address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number
   or
   address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number

5. network ip-address [wildcard-mask]

6. eigrp stub [receive-only] [leak-map name] [connected] [static] [summary] [redistributed]

7. exit-address-family

8. exit

9. exit

10. show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast]
    neighbors [static] [detail] [interface-type interface-number]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 router eigrp virtual-instance-name</td>
<td>Enables an EIGRP routing process in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# router eigrp virtual-name</td>
<td></td>
</tr>
<tr>
<td>Step 4 address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
<td>Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.</td>
</tr>
<tr>
<td>or address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router)# address-family ipv4 autonomous-system 45000</td>
<td></td>
</tr>
<tr>
<td>Step 5 network ip-address [wildcard-mask]</td>
<td>Specifies the network address of the EIGRP distribution router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af)# network 172.16.0.0</td>
<td></td>
</tr>
</tbody>
</table>
## Command or Action

<table>
<thead>
<tr>
<th>Step 6</th>
<th><strong>eigrp stub</strong> [receive-only] [leak-map name] [connected] [static] [summary] [redistributed]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-router-af) eigrp stub leak-map map1</td>
</tr>
</tbody>
</table>

**Purpose**: Configures a router as a stub using EIGRP.

<table>
<thead>
<tr>
<th>Step 7</th>
<th><strong>exit-address-family</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-router-af)# exit-address-family</td>
</tr>
</tbody>
</table>

**Purpose**: Exits address family configuration mode.

<table>
<thead>
<tr>
<th>Step 8</th>
<th><strong>exit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-router)# exit</td>
</tr>
</tbody>
</table>

**Purpose**: Exits to global configuration mode.

<table>
<thead>
<tr>
<th>Step 9</th>
<th><strong>exit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-router)# exit</td>
</tr>
</tbody>
</table>

**Purpose**: Exits to privileged EXEC mode.

| Step 10  | **show eigrp address-family** {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] neighbors [static] [detail] [interface-type interface-number] |
|----------|-------------------------------------------------------------------------------------------------|
| Example: | Router# show eigrp address-family ipv4 neighbors detail                                         |

**Purpose**: (Optional) Displays the neighbors that are discovered by EIGRP.

---

### Monitoring and Maintaining EIGRP: Autonomous System Configuration

Use the following commands to display information about EIGRP AS configurations.

#### SUMMARY STEPS

1. **enable**
2. **show ip eigrp [vrf {vrf-name | *}] [autonomous-system-number] accounting**
3. **show ip eigrp events [starting-event-number ending-event-number] [type]**
4. **show ip eigrp interfaces [vrf {vrf-name | *}] [autonomous-system-number] [type number] [detail]**
5. **show ip eigrp [vrf {vrf-name | *}] [autonomous-system-number] neighbors [interface-type | static | detail]**
6. **show ip eigrp [vrf {vrf-name | *}] [autonomous-system-number] topology [ip-address [mask]] | [name] | [active] | [all-links] | [detail-links] | [pending] | [summary] | [zero-successors]**
7. **show ip eigrp [vrf {vrf-name | *}] [autonomous-system-number] traffic**
Step 1: `enable`
Enables privileged EXEC mode. Enter your password if prompted.
```
Router# enable
```

Step 2: `show ip eigrp [vrf {vrf-name | *}) [autonomous-system-number] accounting`
This command displays prefix accounting information for EIGRP processes. The following is sample output from the command:
```
Router# show ip eigrp vrf VRF1 accounting
EIGRP-IPv4 Accounting for AS(100)/ID(10.0.2.1) VRF(VRF1)
Total Prefix Count: 4 States: A-Adjacency, P-Pending, D-Down
State Address/Source Interface Prefix Restart Restart/Count Count Count Reset(s)
P Redistributed ---- 0 3 211
A 10.0.1.2 Et0/0 2 0 84
F 10.0.2.4 Se2/0 0 2 114
D 10.0.1.3 Et0/0 0 3 0
```

Step 3: `show ip eigrp events [starting-event-number ending-event-number] [type]`
This command displays the EIGRP event log. The following is sample output from the command:
```
Router# show ip eigrp events
1 02:37:58.171 NSF stale rt scan, peer: 10.0.0.0
2 02:37:58.167 Metric set: 10.0.0.1/24 284700416
3 02:37:58.167 FC sat rdbmet/succmet: 284700416 0
4 02:37:58.167 FC sat nh/ndbmet: 10.0.0.2 284700416
5 02:37:58.167 Find FS: 10.0.0.0/24 284700416
6 02:37:58.167 Rcv update met/succmet: 284956416 284700416
7 02:37:58.167 Rcv update dest/nh: 10.0.0.0/24 10.0.0.1
8 02:37:58.167 Peer nsf restarted: 10.0.0.1 Tunnel0
9 02:36:38.383 Metric set: 10.0.0.0/24 284700416
10 02:36:38.383 RDB delete: 10.0.0.0/24 10.0.0.1
11 02:36:38.383 FC sat rdbmet/succmet: 284700416 0
12 02:36:38.383 FC sat nh/ndbmet: 0.0.0.0 284700416
```

Step 4: `show ip eigrp interfaces [vrf {vrf-name | *}) [autonomous-system-number] [type number] [detail]`
This command displays information about interfaces that are configured for EIGRP. The following is sample output from the command:
```
Router# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(60)
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Peers</th>
<th>Xmit Queue Un/Reliable</th>
<th>Mean SRTT</th>
<th>Pacing Time Un/Reliable</th>
<th>Multicast Flow Timer</th>
<th>Pending Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>D10</td>
<td>0</td>
<td>0/0</td>
<td>11/434</td>
<td>0/0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Et0</td>
<td>1</td>
<td>0/0</td>
<td>337</td>
<td>0/10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SE0:1.16</td>
<td>1</td>
<td>0/0</td>
<td>10</td>
<td>1/63</td>
<td>103</td>
<td>0</td>
</tr>
<tr>
<td>Tu0</td>
<td>1</td>
<td>0/0</td>
<td>330</td>
<td>0/16</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Configuring EIGRP

How to Configure EIGRP

Step 5  show ip eigrp [vrf {vrf-name | *}] [autonomous-system-number] neighbors [interface-type | static | detail]

This command displays neighbors discovered by EIGRP. The following is sample output from this command:

```
Router# show ip eigrp neighbors

H  Address           Interface       Hold Uptime  SRTT   RTO  Q  Seq
     (sec)         (ms)       Cnt Num
0   10.1.1.2        Et0/0            13 00:00:03 1996  5000  0  5
2   10.1.1.9        Et0/0            14 00:02:24   206  5000  0  5
1   10.1.2.3        Et0/1            11 00:20:39   2202  5000  0  5
```

Step 6  show ip eigrp [vrf {vrf-name | *}] [autonomous-system-number] topology [ip-address [mask]] | [name] [active | all-links | detail-links | pending | summary | zero-successors]

This command displays entries in the EIGRP topology table. The following is sample output from this command:

```
Router# show ip eigrp topology

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status, s - sia status
P 10.0.0.0/8, 1 successors, FD is 409600
   via 1.1.1.2 (409600/128256), Ethernet0/0
P 172.16.1.0/24, 1 successors, FD is 409600
   via 1.1.1.2 (409600/128256), Ethernet0/0
P 10.0.0.0/8, 1 successors, FD is 281600
   via Summary (281600/0), Null0
P 10.0.1.0/24, 1 successors, FD is 281600
   via Connected, Ethernet0/0
```

Step 7  show ip eigrp [vrf {vrf-name | *}] [autonomous-system-number] traffic

This command displays the number of EIGRP packets sent and received. The following is sample output from the command:

```
Router# show ip eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS(60)
Hellos sent/received: 21429/2809
Updates sent/received: 22/17
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 16/13
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
Hello Process ID: 204
PDM Process ID: 203
Socket Queue: 0/2000/2/0 (current/max/highest/drops)
Input Queue: 0/2000/2/0 (current/max/highest/drops)
```

Monitoring and Maintaining EIGRP: Named Configuration

Use the following commands to display information about EIGRP named configurations.
SUMMARY STEPS

1. enable
2. show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] accounting
3. show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] events [starting-event-number ending-event-number] [errmsg [starting-event-number ending-event-number]] [sia [starting-event-number ending-event-number]] [type]
4. show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] interfaces [detail] [interface-type interface-number]
5. show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] neighbors [static] [detail] [interface-type interface-number]
6. show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] timers
7. show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] topology [topology-name] [ip-address] [active] [all-links] [detail-links] [pending] [summary] [zero-successors] [route-type {connected | external | internal | local | redistributed | summary | vpn}]
8. show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] traffic
9. show eigrp plugins [plugin-name] [detailed]
10. show eigrp protocols [vrf vrf-name]

DETAILED STEPS

Step 1
enable
Enables privileged EXEC mode. Enter your password if prompted.
Router# enable

Step 2
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] accounting
This command displays prefix accounting information for EIGRP processes. The following is sample output from the command:

Router# show eigrp address-family ipv4 22 accounting

EIGRP-IPv4 VR(saf) Accounting for AS(22)/ID(10.0.0.1)
Total Prefix Count: 3 States: A-Adjacency, P-Pending, D-Down

<table>
<thead>
<tr>
<th>State</th>
<th>Address/Source</th>
<th>Interface</th>
<th>Prefix Count</th>
<th>Restart Count</th>
<th>Restart/Reset(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10.0.0.2</td>
<td>Et0/0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>P</td>
<td>10.0.2.4</td>
<td>Se2/0</td>
<td>0</td>
<td>2</td>
<td>114</td>
</tr>
<tr>
<td>D</td>
<td>10.0.1.3</td>
<td>Et0/0</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Step 3
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] events [starting-event-number ending-event-number] [errmsg [starting-event-number ending-event-number]] [sia [starting-event-number ending-event-number]] [type]
This command displays information about EIGRP address-family events. The following is sample output from the command:

```
Router# show eigrp address-family ipv4 3 events
Event information for AS 3:
1 15:37:47.015 Change queue emptied, entries: 1
2 15:37:47.015 Metric set: 10.0.0.0/24 307200
3 15:37:47.015 Update reason, delay: new if 4294967295
4 15:37:47.015 Update sent, RD: 10.0.0.0/24 4294967295
5 15:37:47.015 Update reason, delay: metric chg 4294967295
6 15:37:47.015 Update sent, RD: 10.0.0.0/24 4294967295
7 15:37:47.015 Route installed: 10.0.0.0/24 1.1.1.2
8 15:37:47.015 Route installing: 10.0.0.0/24 10.0.1.2
```

**Step 4**

```
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] interfaces [detail] [interface-type interface-number]
```

This command displays information about interfaces that are configured for EIGRP. The following is sample output from the command:

```
Router# show eigrp address-family ipv4 4453 interfaces
EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Services
Se0 1 0/0 28 0/15 127 0
Se1 1 0/0 44 0/15 211 0
```

**Step 5**

```
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] neighbors [static] [detail] [interface-type interface-number]
```

This command displays the neighbors that are discovered by EIGRP. The following is sample output from the command:

```
Router# show eigrp address-family ipv4 4453 neighbors
EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
Address Interface Hold Uptime SRTT RTO Q Seq
| (sec) | (ms) | (ms) | Cnt | Num
172.16.81.28 Ethernet1 13 0:00:41 0 11 4 20
172.16.80.28 Ethernet0 14 0:02:01 0 10 12 24
172.16.80.31 Ethernet0 12 0:02:02 0 4 5 20
```

**Step 6**

```
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] timers
```

This command displays information about EIGRP timers and expiration times. The following is sample output from the command:

```
Router# show eigrp address-family ipv4 4453 timers
EIGRP-IPv4 VR(Virtual-name) Address-family Timers for AS(4453)
Hello Process
| Expiration Type |
| 1.022 (parent) |
| 1.022 Hello (Et0/0) |
Update Process
| Expiration Type |
| 14.984 (parent) |
| 14.984 (parent) |
| 14.984 Peer holding |
```
Configuring EIGRP

How to Configure EIGRP

<table>
<thead>
<tr>
<th>SIA Process</th>
<th>Expiration Type for Topo(base)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.000 (parent)</td>
</tr>
</tbody>
</table>

**Step 7**

```bash
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast]
topology [topology-name] [ip-address] [active] [all-links] [detail-links] [pending] [summary]
[zero-successors] [route-type {connected | external | internal | local | redistributed | summary | vpn}]
```

This command displays entries in the EIGRP topology table. The following is sample output from the command:

```bash
Router# show eigrp address-family ipv4 4453 topology
```

EIGRP-IPv4 VR(Virtual-name) Topology Table for AS(4453)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status, s - sia Status
P 10.17.17.0/24, 1 successors, FD is 409600
   via 10.10.10.2 (409600/128256), Ethernet3/0
P 172.16.19.0/24, 1 successors, FD is 409600
   via 10.10.10.2 (409600/128256), Ethernet3/0
P 192.168.10.0/24, 1 successors, FD is 281600
   via Connected, Ethernet3/0
P 10.10.10.0/24, 1 successors, FD is 281600
   via Redistributed (281600/0)

**Step 8**

```bash
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast]
traffic
```

This command displays the number of EIGRP packets that are sent and received. The following is sample output from the command:

```bash
Router# show eigrp address-family ipv4 4453 traffic
```

EIGRP-IPv4 VR(virtual-name) Address-family Traffic Statistics for AS(4453)
Hellos sent/received: 122/122
Updates sent/received: 3/1
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 0/3
SIA-Queries sent/received: 0/0
SIA- Replies sent/received: 0/0
Hello Process ID: 128
PDM Process ID: 191
Socket Queue: 0/2000/1/0 (current/max/highest/drops)
Input Queue: 0/2000/1/0 (current/max/highest/drops)

**Step 9**

```bash
show eigrp plugins [plugin-name] [detailed]
```

This command displays general information including the versions of the EIGRP protocol features that are currently running. The following is sample output from the command:

```bash
Router# show eigrp plugins
```

EIGRP feature plugins:::
- eigrp-release : 5.00.00 : Portable EIGRP Release
- igrp2         : 3.00.00 : Reliable Transport/Dual Database
- bfd           : 1.01.00 : BFD Platform Support
- mtr           : 1.00.01 : Multi-Topology Routing (MTR)
- eigrp-pfr     : 1.00.01 : Performance Routing Support
- ipv4-af       : 2.01.01 : Routing Protocol Support
- ipv4-sf       : 1.01.00 : Service Distribution Support
- external-client : 1.02.00 : Service Distribution Client Support
ipv6-af : 2.01.01 : Routing Protocol Support
ipv6-sf : 1.01.00 : Service Distribution Support
snmp-agent : 1.01.01 : SNMP/SNMPv2 Agent Support

**Step 10**  *show eigrp protocols [vrf vrf-name]*

This command displays general information about EIGRP protocols that are currently running. The following is sample output from the command:

```
Router# show eigrp protocols
EIGRP-IPv4 Protocol for AS(10)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 1.1.1.1
Topology: 0 (base)
Distance: internal 90 external 170
Active Timer: 3 min
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
EIGRP-IPv4 Protocol for AS(5) VRF(VRF1)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 1.1.1.1
Topology: 0 (base)
Distance: internal 90 external 170
Active Timer: 3 min
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
Total Prefix Count: 0
Total Redist Count: 0
```

---

**Configuration Examples for EIGRP**

This section provides the following configuration examples for EIGRP:

- Enabling EIGRP: Autonomous System Configuration Example, page 55
- Enabling EIGRP: Named Configuration Example, page 55
- EIGRP Parameters: Autonomous System Configuration Example, page 55
- EIGRP Parameters: Named Configuration Example, page 55
- EIGRP Redistribution: Autonomous System Configuration Example, page 56
- EIGRP Redistribution: Named Configuration Example, page 56
- EIGRP Route Summarization: Autonomous System Configuration Example, page 56
- EIGRP Route Summarization: Named Configuration Example, page 57
- EIGRP Event Logging: Autonomous System Configuration Example, page 57
- EIGRP Event Logging: Named Configuration Example, page 57
- Equal and Unequal Cost Load Balancing: Autonomous System Configuration Example, page 58
- Equal and Unequal Cost Load Balancing: Named Configuration Example, page 58
- EIGRP Route Authentication: Autonomous System Configuration Example, page 58
Enabling EIGRP: Autonomous System Configuration Example

The following example shows how to enable EIGRP in AS configurations:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 1
Router(config-router)# network 172.16.0.0
```

Enabling EIGRP: Named Configuration Example

The following example shows how to enable EIGRP in named configurations:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# network 172.16.0.0
```

EIGRP Parameters: Autonomous System Configuration Example

The following example shows how to configure optional EIGRP AS configuration parameters including applying offsets to routing metrics, adjusting EIGRP metrics, and disabling automatic summarization:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 1
Router(config-router)# network 172.16.0.0
Router(config-router)# passive-interface
Router(config-router)# offset-list 21 in 10 ethernet 0
Router(config-router)# metric weights 0 2 0 2 0 0
Router(config-router)# no auto-summary
Router(config-router)# exit
```

EIGRP Parameters: Named Configuration Example

The following example shows how to configure optional EIGRP named configuration parameters including applying offsets to routing metrics, adjusting EIGRP metrics, and disabling automatic summarization.
**EIGRP Redistribution: Autonomous System Configuration Example**

The following example shows how to configure redistribution of non-EIGRP protocol metrics into EIGRP metrics and to configure the EIGRP administrative distance in an EIGRP AS configuration:

```plaintext
Router> enable
Router# configure terminal
Router(config)# router eigrp 1
Router(config-router)# network 172.16.0.0
Router(config-router)# redistribute rip
Router(config-router)# distance eigrp 80 130
Router(config-router)# default-metric 1000 100 250 100 1500
```

**EIGRP Redistribution: Named Configuration Example**

The following example shows how to configure redistribution of non-EIGRP protocol metrics into EIGRP metrics and to configure the EIGRP administrative distance in an EIGRP named configuration:

```plaintext
Router> enable
Router# configure terminal
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af)# passv-interface
Router(config-router-af)# bandwidth-percent 75
Router(config-router-af)# exit-af-interface
Router(config-router-af)# topology base
Router(config-router-af-topology)# offset-list 21 in 10 ethernet 0
Router(config-router-af-topology)# no auto-summary
Router(config-router-af-topology)# exit-af-topology
```

**EIGRP Route Summarization: Autonomous System Configuration Example**

The following example configures route summarization on an interface and also configures the automatic summary feature for an EIGRP AS configuration. This configuration causes EIGRP to summarize network 10.0.0.0 out Ethernet interface 0 only.

```plaintext
Router> enable
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# exit
Router(config)# interface ethernet0
```
You should not use the `ip summary-address eigrp` summarization command to generate the default route (0.0.0.0) from an interface. This causes the creation of an EIGRP summary default route to the null 0 interface with an administrative distance of 5. The low administrative distance of this default route can cause this route to displace default routes learned from other neighbors from the routing table. If the default route learned from the neighbors is displaced by the summary default route, or if the summary route is the only default route present, all traffic destined for the default route will not leave the router, instead, this traffic will be sent to the null 0 interface, where it is dropped.

The recommended way to send only the default route out a given interface is to use a `distribute-list` command. You can configure this command to filter all outbound route advertisements sent out the interface with the exception of the default (0.0.0.0).

---

**EIGRP Route Summarization: Named Configuration Example**

The following example configures route summarization on an interface and also configures the automatic summary feature for an EIGRP named configuration. This configuration causes EIGRP to summarize network 192.168.0.0 out Ethernet interface 0/0 only.

```plaintext
Router> enable
Router# configure terminal
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# summary-address 192.168.0.0 255.255.0.0
```

**EIGRP Event Logging: Autonomous System Configuration Example**

The following example shows how to configure EIGRP event logging parameters for an EIGRP AS configuration:

```plaintext
Router> enable
Router# configure terminal
Router(config)# router eigrp 1
Router(config-router)# eigrp event-log-size 5000
Router(config-router)# eigrp log-neighbor-changes
Router(config-router)# eigrp log-neighbor-warnings 300
```

**EIGRP Event Logging: Named Configuration Example**

The following example shows how to configure EIGRP event logging parameters, including setting the size of the EIGRP event log, for an EIGRP named configuration:

```plaintext
Router> enable
Router# configure terminal
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# eigrp log-neighbor-warnings 300
Router(config-router-af)# eigrp log-neighbor-changes
Router(config-router-af)# topology base
```
Equal and Unequal Cost Load Balancing: Autonomous System Configuration Example

The following example shows how to configure traffic distribution among routes, the maximum number of parallel routes, and load balancing in an EIGRP named configuration network:

Router> enable
Router# configure terminal
Router(config)# router eigrp 1
Router(config-router)# traffic-share balanced
Router(config-router)# maximum-paths 5
Router(config-router)# variance 1

EIGRP Route Authentication: Autonomous System Configuration Example

The following example enables MD5 authentication on EIGRP packets in autonomous system 1. Figure 7 shows the scenario.

Figure 7  EIGRP Route Authentication Scenario

Enhanced IGRP Autonomous System 1

Router A Configuration

Router> enable
Router(config)# configure terminal
Router(config)# router eigrp 1
Router(config-router)# exit
Router(config)# interface ethernet 1
Router(config-if)# ip authentication mode eigrp 1 md5
Router(config-if)# ip authentication key-chain eigrp 1 key1
Router(config-if)# exit
Router(config)# key chain key1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string 0987654321
Router(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Router(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 04:48:00 Dec 4 1996
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string 1234567890
Router(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Router(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite

Router(config)# key chain key2
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string 0987654321
Router(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Router(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string 1234567890
Router(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Router(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite

Router A will accept and attempt to verify the MD5 digest of any EIGRP packet with a key equal to 1. It will also accept a packet with a key equal to 2. All other MD5 packets will be dropped. Router A will send all EIGRP packets with key 2.

Router B will accept key 1 or key 2, and will use key 1 to send MD5 authentication, because key 1 is the first the first valid key off the key-chain. Key 1 will no longer be valid to be used for sending after December 4, 2006. After this date, key 2 would be used to send MD5 authentication, because it is valid until January 4, 2007.

EIGRP Route Authentication: Named Configuration Example

The following example enables MD5 authentication on EIGRP packets in a named configuration. Figure 7 shows the scenario.

Router A Configuration

Router> enable
Router# configure terminal
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain SITE1
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit-af-interface
Router(config-router-af)# exit-address-family
Router(config-router)# exit
Router(config)# key chain SITE1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string 0987654321
Router(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Router(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string 1234567890
Router(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Router(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite

Router B Configuration
Router> enable
Router# configure terminal
Router(config)# router eigrp virtual-name2
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af)# authentication key-chain SITE2
Router(config-router-af)# authentication mode md5
Router(config-router-af)# exit-af-interface
Router(config-router-af)# exit-address-family
Router(config-router)# exit
Router(config)# key chain SITE2
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string 0987654321
Router(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Router(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite

Router A will accept and attempt to verify the MD5 digest of any EIGRP packet with a key equal to 1. It will also accept a packet with a key equal to 2. All other MD5 packets will be dropped. Router A will send all EIGRP packets with key 2.

Router B will accept key 1 or key 2, and will use key 1 to send MD5 authentication, because key 1 is the first valid key off the key-chain. Key 1 will no longer be valid to be used for sending after December 4, 2006. After this date key 2 would be used to send MD5 authentication, because it is valid until January 4, 2007.

Adjusting the Interval Between Hello Packets and the Hold Time: Autonomous System Configuration Example

The following example shows how to adjust the interval between hello packets and the hold time in an EIGRP AS configuration:

Router> enable
Router# configure terminal
Router(config)# router eigrp 1
Router(config-router)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# ip hello-interval eigrp 109 10
Router(config-if)# ip hold-time eigrp 109 40
Adjusting the Interval Between Hello Packets and the Hold Time: Named Configuration Example

The following example shows how to adjust the interval between hello packets and the hold time in an EIGRP named configuration:

Router> enable
Router# configure terminal
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# hello-interval 10
Router(config-router-af-interface)# hold-time 50

Disabling Split Horizon: Autonomous System Configuration Example

Split horizon is enabled on all interfaces by default. The following example shows how to disable split horizon for an EIGRP AS configuration:

Router> enable
Router# configure terminal
Router(config)# router eigrp 1
Router(config-router)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# no ip split-horizon eigrp 101

Disabling Split Horizon and Next-Hop-Self: Named Configuration Example

Split horizon is enabled on all interfaces by default. The following example shows how to disable split horizon in an EIGRP named configuration.

EIGRP will, by default, set the next-hop value to the local outbound interface address for routes that it is advertising, even when advertising those routes back out the same interface where it learned them. The following example shows how to change this default to instruct EIGRP to use the received next hop value when advertising these routes in an EIGRP named configuration. Disabling next-hop-self is primarily useful in Dynamic Multipoint VPN (DMVPN) spoke-to-spoke topologies.

Router> enable
Router# configure terminal
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# af-interface ethernet0/0
Router(config-router-af-interface)# no split-horizon
Router(config-router-af-interface)# no next-hop-self eigrp

EIGRP Stub Routing: Autonomous System Configuration Example

A router that is configured as a stub with the eigrp stub command shares connected and summary routing information with all neighbor routers by default. Six keywords can be used with the eigrp stub command to modify this behavior:

- receive-only
- leak-map
- connected
- static
- summary
- redistributed

This section provides configuration examples for all forms of the `eigrp stub` command for an EIGRP AS configuration.

**eigrp stub Command: Example**

In the following example, the `eigrp stub` command is used to configure the router as a stub that advertises connected and summary routes:

```config
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# eigrp stub
```

**eigrp stub connected static Command: Example**

In the following example, the `eigrp stub` command is issued with the `connected` and `static` keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```config
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# eigrp stub connected static
```

**eigrp stub receive-only Command: Example**

In the following example, the `eigrp stub` command is issued with the `receive-only` keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```config
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# eigrp stub receive-only
```

**eigrp stub redistributed Command: Example**

In the following example, the `eigrp stub` command is issued with the `redistributed` keyword to configure the router to advertise other protocols and autonomous systems:

```config
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# eigrp stub redistributed
```

**eigrp stub leak-map Command: Example**

In the following example, the `eigrp stub` command is issued with the `leak-map name` keyword and argument pair to configure the router to reference a leak map that identifies routes that would have been suppressed:

```config
Router(config)# router eigrp
Router(config-router)# network 10.0.0.0
Router(config-router) eigrp stub leak-map map1
```
EIGRP Stub Routing: Named Configuration Example

A router that is configured as a stub with the `eigrp stub` command shares connected and summary routing information with all neighbor routers by default. Six keywords can be used with the `eigrp stub` command to modify this behavior:

- receive-only
- leak-map
- connected
- static
- summary
- redistributed

This section provides configuration examples for all forms of the `eigrp stub` command for an EIGRP named configuration.

`eigrp stub` Command: Example

In the following example, the `eigrp stub` command is used to configure the router as a stub that advertises connected and summary routes:

```config
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub
```

`eigrp stub connected static` Command: Example

In the following named configuration example, the `eigrp stub` command is issued with the `connected` and `static` keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```config
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub connected static
```

`eigrp stub receive-only` Command: Example

In the following named configuration example, the `eigrp stub` command is issued with the `receive-only` keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```config
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub receive-only
```

`eigrp stub redistributed` Command: Example

In the following named configuration example, the `eigrp stub` command is issued with the `redistributed` keyword to configure the router to advertise other protocols and autonomous systems:

```config
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub redistributed
```
eigrp stub leak-map Command: Example
In the following named configuration example, the eigrp stub command is issued with the leak-map name keyword and argument pair to configure the router to reference a leak map that identifies routes that would normally have been suppressed:

```
Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af) eigrp stub leak-map map1
```

Additional References
The following sections provide references related to the EIGRP.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP message authentication</td>
<td>EIGRP Message Authentication Configuration Example</td>
</tr>
<tr>
<td>EIGRP commands</td>
<td>“EIGRP Commands” chapter of the Cisco IOS IP Routing: EIGRP Command Reference</td>
</tr>
<tr>
<td>Protocol-independent features that work with EIGRP</td>
<td>Configuring IP Routing Protocol-Independent Features</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Command Lookup Tool</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>EIGRP L2/L3 API and Tunable Metric for Mobile Adhoc Networks feature</td>
<td>EIGRP L2/L3 API and Tunable Metric for Mobile Adhoc Networks</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Feature Information for EIGRP

Table 3 lists the features in this module and provides links to specific configuration information. Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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

Note

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

Table 3  Feature Information for EIGRP Features

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Interior Gateway Routing Protocol</td>
<td>11.2(1)</td>
<td>EIGRP is an enhanced version of the IGRP developed by Cisco. EIGRP uses the same distance vector algorithm and distance information as IGRP. However, the convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP, and IGRP is obsolete. The following commands were introduced or modified by this feature: auto-summary (EIGRP), clear ip eigrp neighbors, default-information, default-metric (EIGRP), distance (EIGRP), eigrp log-neighbor-changes, eigrp log-neighbor-warnings, eigrp router-id, ip bandwidth-percent eigrp, ip hello-interval eigrp, ip hold-time eigrp, ip next-hop-self eigrp, ip split-horizon eigrp, ip summary-address eigrp, metric maximum-hops, metric weights (EIGRP), neighbor (EIGRP), network (EIGRP), offset-list (EIGRP), redistribute maximum-prefix (EIGRP), router eigrp, set metric (EIGRP), show ip eigrp accounting, show ip eigrp interfaces, show ip eigrp neighbors, show ip eigrp topology, show ip eigrp traffic, show ip eigrp vrf accounting, show ip eigrp vrf interfaces, show ip eigrp vrf neighbors, show ip eigrp vrf topology, show ip eigrp vrf traffic, timers active-time, traffic-share balanced, variance (EIGRP).</td>
</tr>
<tr>
<td>(EIGRP)</td>
<td>12.2(33)SRA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15.0(1)M</td>
<td></td>
</tr>
</tbody>
</table>
Table 3  Feature Information for EIGRP Features (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS Release 15.0(1)M, the following commands were introduced or modified: address-family (EIGRP), af-interface, autonomous-system (EIGRP), auto-summary (EIGRP), bandwidth percent, clear eigrp address-family neighbors, clear ip eigrp neighbors, debug eigrp address-family neighbor, debug eigrp address-family notifications, default-information, default-metric (EIGRP), distance (EIGRP), eigrp event-log-size, eigrp log-neighbor-changes, eigrp log-neighbor-warnings, eigrp router-id, exit-address-family, exit-af-interface, exit-af-topology, hello-interval, hold-time, match extcommunity, metric maximum-hops, metric weights, next-hop-self, offset-list (EIGRP), passive-interface (EIGRP), router eigrp, show eigrp address-family accounting, show eigrp address-family events, show eigrp address-family interfaces, show eigrp address-family neighbors, show eigrp address-family timers, show eigrp address-family topology, show eigrp address-family traffic, show eigrp plugins, show eigrp protocols, show eigrp tech-support, show ip eigrp accounting, show ip eigrp events, show ip eigrp interfaces, show ip eigrp neighbors, show ip eigrp topology, show ip eigrp traffic, shutdown (address-family), split-horizon (EIGRP), summary-address (EIGRP), timers active-time, traffic-share balanced, variance (EIGRP).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS Release 15.0(1)M, the following commands were replaced: clear ip eigrp vrf neighbors, eigrp interface, log-neighbor-warnings, show ip eigrp vrf accounting, show ip eigrp vrf interfaces, show ip eigrp vrf neighbors, show ip eigrp vrf topology, show ip eigrp vrf traffic.</td>
</tr>
</tbody>
</table>
Configuring EIGRP

Table 3  Feature Information for EIGRP Features (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP Stub Routing</td>
<td>12.0(7)T</td>
<td>The EIGRP Stub Routing feature improves network stability, reduces resource utilization, and simplifies stub router configuration. Stub routing is</td>
</tr>
<tr>
<td></td>
<td>12.0(15)S</td>
<td>commonly used in a hub-and-spoke network topology. In a hub-and-spoke network, one or more end (stub) networks are connected to a remote router (the</td>
</tr>
<tr>
<td></td>
<td>15.0(1)M</td>
<td>spoke) that is connected to one or more distribution routers (the hub). The remote router is adjacent only to one or more distribution routers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following sections provide information about this feature:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EIGRP Stub Routing, page 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EIGRP Stub Routing Leak Map Support, page 16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuring EIGRP Stub Routing: Autonomous System Configuration, page 45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuring EIGRP Stub Routing: Named Configuration, page 46</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EIGRP Stub Routing: Autonomous System Configuration Example, page 61</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EIGRP Stub Routing: Named Configuration Example, page 63</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following command was introduced by this feature:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eigrp stub.</td>
</tr>
</tbody>
</table>
Table 3  Feature Information for EIGRP Features (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Enhanced IGRP Route Authentication</td>
<td>11.3(1)</td>
<td>The IP Enhanced IGRP route authentication feature provides MD5 authentication of routing updates from the EIGRP routing protocol.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15.0(1)M</td>
<td>The following sections provide information about this feature:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- EIGRP Route Authentication, page 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configuring EIGRP Route Authentication: Autonomous System Configuration, page 35</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configuring EIGRP Route Authentication: Named Configuration, page 37</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- EIGRP Route Authentication: Autonomous System Configuration Example, page 58</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- EIGRP Route Authentication: Named Configuration Example, page 59</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced or modified by this feature: accept-lifetime, ip authentication key-chain eigrp, ip authentication mode eigrp, key chain, key, key-string, send-lifetime</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS Release 15.0(1)M, the following commands were introduced or modified: authentication mode (EIGRP), authentication key-chain (EIGRP)</td>
</tr>
</tbody>
</table>
EIGRP Nonstop Forwarding (NSF) Awareness

First Published: April 26, 2005
Last Updated: October 2, 2009

Nonstop Forwarding (NSF) awareness allows an NSF-aware router to assist NSF-capable and NSF-aware neighbors to continue forwarding packets during a switchover operation or during a well-known failure condition. The EIGRP Nonstop Forwarding Awareness feature allows an NSF-aware router that is running Enhanced Interior Gateway Routing Protocol (EIGRP) to forward packets along routes known to a router performing a switchover operation or in a well-known failure condition. This capability allows the EIGRP peers of the failing router to retain the routing information that it has advertised and to continue using this information until the failed router resumes normal operation and is able to exchange routing information. The peering session is maintained throughout the entire NSF operation.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information for EIGRP Nonstop Forwarding Awareness, page 11

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

Contents

- Prerequisites for EIGRP Nonstop Forwarding Awareness, page 2
- Restrictions for EIGRP Nonstop Forwarding Awareness, page 2
- Information About EIGRP Nonstop Forwarding Awareness, page 2
- How to Modify and Maintain EIGRP Nonstop Forwarding Awareness, page 5
Prerequisites for EIGRP Nonstop Forwarding Awareness

- Your network is configured to run EIGRP.
- An NSF-aware router must be up and completely converged with the network before it can assist an NSF-capable router in an NSF restart operation.
- A version of Cisco IOS that supports NSF awareness or NSF capabilities must be installed.

Restrictions for EIGRP Nonstop Forwarding Awareness

- All neighboring devices participating in EIGRP NSF must be NSF-capable or NSF-aware.
- EIGRP NSF awareness does not support two neighbors performing an NSF restart operation at the same time. However, both neighbors can reestablish peering sessions after the NSF restart operation is completed.

Information About EIGRP Nonstop Forwarding Awareness

To configure this feature, you should understand the following concepts:

- Cisco NSF Routing and Forwarding Operation, page 2
- Cisco Express Forwarding, page 3
- EIGRP Nonstop Forwarding Awareness, page 3
- EIGRP NSF Capable and NSF Aware Interoperation, page 4
- Non-NSF Aware EIGRP Neighbors, page 4
- EIGRP NSF Route-Hold Timers

Cisco NSF Routing and Forwarding Operation

Cisco NSF is supported by the BGP, EIGRP, OSPF, and IS-IS protocols for routing and by Cisco Express Forwarding (CEF) for forwarding. Of the routing protocols, BGP, OSPF, and IS-IS have been enhanced with NSF-capability and awareness, which means that routers running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices. The IS-IS protocol can be configured to use state information that has been synchronized between the active and the standby route processor (RP) to recover route information following a switchover instead of information received from peer devices.

In this document, a networking device that is NSF-aware is running NSF-compatible software. A device that is NSF-capable has been configured to support NSF; therefore, the device rebuilds routing information from NSF-aware or NSF-capable neighbors.
EIGRP Nonstop Forwarding (NSF) Awareness

Information About EIGRP Nonstop Forwarding Awareness

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the routing information base (RIB) tables. After the routing protocols have converged, CEF updates the forwarding information base (FIB) table and removes stale route entries. CEF, in turn, updates the line cards with the new FIB information.

Cisco Express Forwarding

In a Cisco networking device, CEF provides packet forwarding, a key element of NSF. CEF maintains the FIB and uses the FIB information that was current at the time of a switchover to continue forwarding packets during the switchover. NSF helps to reduce traffic interruption during the switchover.

During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards will maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF will keep the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates for CEF, which it uses to update the FIB and adjacency databases. Existing and new entries will receive the new version (“epoch”) number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engine during convergence. The RP signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

The routing protocols run only on the active RP, and they receive routing updates from their neighbor routers. Routing protocols do not run on the standby RP. Following a switchover, the routing protocols request that the NSF-aware neighbor devices send state information to help rebuild the routing tables.

Note

For NSF operation, the routing protocols depend on CEF to continue forwarding packets while the routing protocols rebuild the routing information.

EIGRP Nonstop Forwarding Awareness

NSF awareness allows a router that is running EIGRP to assist NSF-capable neighbors to continue forwarding packets during a switchover operation or well-known failure condition. The EIGRP Nonstop Forwarding Awareness feature provides EIGRP with the capability to detect a neighbor that is undergoing an NSF restart event (RP switchover operation) or well-known failure condition, maintain the peering session with this neighbor, retain known routes, and continue to forward packets for these routes. The deployment of EIGRP NSF awareness can minimize the effects of the following:

- Well-known failure conditions (for example, a stuck-in-active event)
- Unexpected events (for example, an RP switchover operation)
- Scheduled events (for example, a hitless software upgrade)
EIGRP NSF awareness is enabled by default and is transparent to the network operator and EIGRP peers that do not support NSF capabilities.

**Note**  
An NSF-aware router must be up and completely converged with the network before it can assist an NSF-capable router in an NSF restart operation.

**EIGRP NSF Capable and NSF Aware Interoperation**

EIGRP NSF capabilities are exchanged by EIGRP peers in hello packets. An NSF-capable router notifies its neighbors that an NSF restart operation has started by setting the restart (RS) bit in a hello packet. When an NSF-aware router receives notification from an NSF-capable neighbor that an NSF-restart operation is in progress, both routers immediately exchange their topology tables. The NSF-aware router sends an end-of-table (EOT) update packet when the transmission of its topology table is complete. The NSF-aware router then performs the following actions to assist the NSF-capable router:

- Expires the EIGRP hello hold timer to reduce the time interval set for hello packet generation and transmission. This allows the NSF-aware router to reply to the NSF-capable router more quickly and reduces the amount of time required for the NSF-capable router to rediscover neighbors and rebuild the topology table.
- Starts the route-hold timer. This timer is used to set the period of time that the NSF-aware router will hold known routes for the NSF-capable neighbor. This timer is configured with the `timers graceful-restart purge-time` command. The default time period is 240 seconds.
- Notes in the peer list that the NSF-capable neighbor is restarting, maintains adjacency, and holds known routes for the NSF-capable neighbor until the neighbor signals that it is ready for the NSF-aware router to send its topology table or the route-hold timer expires. If the route-hold timer expires on the NSF-aware router, it discards held routes and treats the NSF-capable router as a new router joining the network and reestablishing adjacency accordingly.

When the switchover operation is complete, the NSF-capable router notifies its neighbors that it has reconverged and has received all of their topology tables by sending an EOT update packet to the assisting routers. The NSF-capable router then returns to normal operation. The NSF-aware router looks for alternate paths (go active) for any routes that are not refreshed by the NSF-capable (restarting) router. The NSF-aware router returns to normal operation. If all paths are refreshed by the NSF-capable router, the NSF-aware router immediately returns to normal operation.

**Non-NSF Aware EIGRP Neighbors**

NSF-aware routers are completely compatible with non-NSF aware or non-NSF capable neighbors in an EIGRP network. A non-NSF aware neighbor ignores NSF capabilities and resets the adjacency when they are received.

The NSF-capable router drops any queries that are received while converging to minimize the number of transient routes that are sent to neighbors. The NSF-capable router, however, still acknowledges these queries to prevent these neighbors from resetting adjacency.

**Note**  
An NSF-aware router continues to send queries to an NSF-capable router that is converging after a switchover, effectively extending the time before a stuck-in-active (SIA) condition can occur.
EIGRP NSF Route-Hold Timers

The route-hold timer is configurable, which allows you to tune network performance and avoid undesired conditions such as “black holing” routes if the switchover operation is lengthy. When the timer expires, the NSF-aware router scans the topology table and discards stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

The route-hold timer is configured with the `timers graceful-restart purge-time` router configuration command. The default time period for the route-hold timer is 240 seconds. The configurable range is from 10 to 300 seconds.

How to Modify and Maintain EIGRP Nonstop Forwarding Awareness

This section contains the following procedures for configuring the EIGRP Nonstop Forwarding Awareness feature:

- Adjusting NSF Route-Hold Timers, page 5
- Monitoring EIGRP NSF Debug Events and Notifications, page 6
- Verifying the Local Configuration of EIGRP NSF Awareness, page 7

Adjusting NSF Route-Hold Timers

Perform the following steps to configure NSF route-hold timers on an NSF-aware router.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `router eigrp {autonomous-system-number | virtual-instance-name}`
4. `timers graceful-restart purge-time seconds`
5. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
On Nonstop Forwarding (NSF) Awareness

Troubleshooting Tips

Neighbor adjacencies are maintained during NSF switchover operations. If adjacencies between NSF-capable and NSF-aware neighbors are being reset too often, the route-hold timers may need to be adjusted. The `show ip eigrp neighbors detail` command can be used to help determine if the route-hold timer value should be set to a longer time period. The time that adjacency is established with specific neighbors is displayed in the output. This time indicates if adjacencies are being maintained or reset and the last time that specific neighbors were restarted.

Monitoring EIGRP NSF Debug Events and Notifications

Perform the following steps to monitor EIGRP NSF debug events and notifications on an NSF-aware router.

Debug Commands

The `debug eigrp nsf` and `debug ip eigrp notifications` commands are provided together for example purposes only. You do not have to issue these commands together or in the same session as there are differences in the information that is provided.

Debugging processes are heavy users of CPU resources. Debug commands should not be used in a production network unless you are troubleshooting a problem.

SUMMARY STEPS

1. `enable`
2. `debug eigrp nsf`
3. `debug eigrp ip notifications`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> debug eigrp nsf</td>
<td>Displays NSF notifications and information about NSF events in an EIGRP network on the console of the router.</td>
</tr>
<tr>
<td>Example: Router# debug eigrp nsf</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> debug ip eigrp notifications</td>
<td>Displays EIGRP events and notifications in the console of the router. The output from this command also includes NSF notifications and information about NSF events.</td>
</tr>
<tr>
<td>Example: Router# debug ip eigrp notifications</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the Local Configuration of EIGRP NSF Awareness

Perform the following steps to verify NSF-awareness configuration on a router that is running EIGRP.

SUMMARY STEPS

1. enable
2. show ip protocols

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show ip protocols</td>
<td>Displays the parameters and current state of the active routing protocol process. The output of this command can be used to verify EIGRP NSF-awareness.</td>
</tr>
<tr>
<td>Example: Router# show ip protocols</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for EIGRP Nonstop Forwarding Awareness

- EIGRP Graceful-Restart Purge-Time Timer Configuration: Example, page 8
- Monitoring EIGRP NSF Debug Events and Notifications Configuration: Example, page 8
- Verifying Local Configuration of EIGRP NSF Awareness: Example, page 8

EIGRP Graceful-Restart Purge-Time Timer Configuration: Example

The `timers graceful-restart purge-time` command is used to set the route-hold timer that determines how long an NSF-aware router that is running EIGRP will hold routes for an inactive peer. The following example shows how to set the route-hold timer to two minutes:

```
Router(config-router)# timers graceful-restart purge-time 120
```

Monitoring EIGRP NSF Debug Events and Notifications Configuration: Example

The following example output shows that an NSF-aware router has received a restart notification. The NSF-aware router waits for EOT to be sent from the restarting (NSF-capable) neighbor.

```
Router# debug ip eigrp notifications
*Oct  4 11:39:18.092:EIGRP:NSF:AS2. Rec RS update from 135.100.10.1, 00:00:00. Wait for EOT.
*Oct  4 11:39:18.092:%DUAL-5-NBRCHANGE:IP-EIGRP(0) 2:Neighbor 135.100.10.1 (POS3/0) is up:peer NSF restarted
*Sep 23 18:49:07.578: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 1.1.2.1 (Ethernet1/0) is resync: peer graceful-restart
```

Verifying Local Configuration of EIGRP NSF Awareness: Example

The following is example output from the `show ip protocols` command. The output from this command can be used to verify the local configuration of EIGRP NSF awareness. The output shows that the router is NSF-aware and that the route-hold timer is set to 240 seconds, which is the default value.

```
Router# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is “eigrp 101”
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Default networks flagged in outgoing updates
    Default networks accepted from incoming updates
    EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    EIGRP maximum hopcount 100
    EIGRP maximum metric variance 1
    Redistribution: eigrp 101
    EIGRP NSF-aware route hold timer is 240s
```
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.4.9.0/24
Routing Information Sources:
  Gateway  Distance  Last Update
  Distance: internal 90  external 170

Additional References

The following sections provide references related to the EIGRP Nonstop Forwarding Awareness feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF commands</td>
<td>Cisco IOS IP Switching Command Reference</td>
</tr>
<tr>
<td>EIGRP commands</td>
<td>Cisco IOS IP Routing: EIGRP Command Reference</td>
</tr>
<tr>
<td>NSF with SSO deployment</td>
<td>Cisco Nonstop Forwarding with Stateful Switchover Deployment Guide</td>
</tr>
<tr>
<td>Master list of Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards</td>
<td>are supported by this feature, and support for existing standards</td>
</tr>
<tr>
<td></td>
<td>has not been modified by this feature.</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 4724</td>
<td>Graceful Restart Mechanism for BGP</td>
</tr>
</tbody>
</table>
## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Feature Information for EIGRP Nonstop Forwarding Awareness

Table 1 lists the release history for this feature.

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

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

Note

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| EIGRP Nonstop Forwarding (NSF) Awareness | 12.2(15)T, 15.0(1)M | The EIGRP Nonstop Forwarding Awareness feature allows an NSF-aware router running EIGRP to forward packets along routes known to a router performing a switchover operation or in a well-known failure condition. The following commands were introduced or modified: `<debug eigrp nsf`, `<debug ip eigrp notifications`, `<show ip eigrp neighbors`, `<show ip protocols`, `<timers graceful-restart`, `<purge-time`, `<timers nsf route-hold>`.

---

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.
The EIGRP MPLS VPN PE-CE Site of Origin feature introduces the capability to filter Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) traffic on a per-site basis for Enhanced Interior Gateway Routing Protocol (EIGRP) networks. Site of Origin (SoO) filtering is configured at the interface level and is used to manage MPLS VPN traffic and to prevent transient routing loops from occurring in complex and mixed network topologies. This feature is designed to support the MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE) feature. Support for backdoor links is provided by this feature when a Cisco IOS release is implemented on PE routers that support EIGRP MPLS VPNs.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for MPLS VPN PE-CE Site of Origin (SoO)” section on page 11. Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

- Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin, page 2
- Restrictions for EIGRP MPLS VPN PE-CE Site of Origin, page 2
- Information About EIGRP MPLS VPN PE-CE Site of Origin, page 2
- How to Configure EIGRP MPLS VPN PE-CE Site of Origin Support, page 5
- Configuration Examples for EIGRP MPLS VPN PE-CE SoO, page 8
- Additional References, page 9
Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin

This document assumes that Border Gateway Protocol (BGP) is configured in the network core (or the service provider backbone). The following tasks will also need to be completed before you can configure this feature:

- This feature was introduced to support the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature and should be configured after the EIGRP MPLS VPN is created.
- All PE routers that are configured to support the EIGRP MPLS VPN must run a Cisco IOS release that provides support for the SoO extended community.

Restrictions for EIGRP MPLS VPN PE-CE Site of Origin

- If a VPN site is partitioned and the SoO extended community attribute is configured on a backdoor router interface, the backdoor link cannot be used as an alternate path to reach prefixes originated in other partitions of the same site.
- A unique SoO value must be configured for each individual VPN site. The same value must be configured on all provider edge and customer edge interfaces (if SoO is configured on the CE routers) that support the same VPN site.

Information About EIGRP MPLS VPN PE-CE Site of Origin

To configure this feature, you must understand the following concepts:

- EIGRP MPLS VPN PE-CE Site of Origin Support Overview, page 2
- Site of Origin Support for Backdoor Links, page 3
- Router Interoperation with a Site of Origin Extended Community, page 3
- Redistribution of BGP VPN Routes That Carry the Site of Origin into EIGRP, page 4
- BGP Cost Community Support for EIGRP MPLS VPN PE-CE Network Topologies, page 4
- Benefits of the EIGRP MPLS VPN PE-CE Site of Origin Support Feature, page 4

EIGRP MPLS VPN PE-CE Site of Origin Support Overview

The EIGRP MPLS VPN PE-CE Site of Origin feature introduces SoO support for EIGRP-to-BGP and BGP-to-EIGRP redistribution. The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the readvertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a PE router has learned a route. SoO support provides the capability to filter MPLS VPN traffic on a per-EIGRP-site basis. SoO filtering is configured at the interface level and is used to manage MPLS VPN traffic and to prevent routing loops from occurring in complex and mixed network topologies, such as EIGRP VPN sites that contain both VPN and backdoor links.

The configuration of the SoO extended community allows MPLS VPN traffic to be filtered on a per-site basis. The SoO extended community is configured in an inbound BGP route map on the PE router and is applied to the interface. The SoO extended community can be applied to all exit points at the customer site for more specific filtering but must be configured on all interfaces of PE routers that provide VPN services to CE routers.
Site of Origin Support for Backdoor Links

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces support for backdoor links. A backdoor link or a route is a connection that is configured outside of the VPN between a remote and main site; for example, a WAN leased line that connects a remote site to the corporate network. Backdoor links are typically used as back up routes between EIGRP sites if the VPN link is down or not available. A metric is set on the backdoor link so that the route though the backdoor router is not selected unless there is a VPN link failure.

The SoO extended community is defined on the interface of the backdoor router. It identifies the local site ID, which should match the value that is used on the PE routers that support the same site. When the backdoor router receives an EIGRP update (or reply) from a neighbor across the backdoor link, the router checks the update for an SoO value. If the SoO value in the EIGRP update matches the SoO value on the local backdoor interface, the route is rejected and not added to the EIGRP topology table. This typically occurs when the route with the local SoO value in the received EIGRP update was learned by the other VPN site and then advertised through the backdoor link by the backdoor router in the other VPN site. SoO filtering on the backdoor link prevents transient routing loops from occurring by filtering out EIGRP updates that contain routes that carry the local site ID.

Note

If a VPN site is partitioned and the SoO extended community attribute is configured on a backdoor router interface, the backdoor link cannot be used as an alternate path to reach prefixes originated in other partitions of the same site.

If this feature is enabled on the PE routers and the backdoor routers in the customer sites, and SoO values are defined on both the PE and backdoor routers, both the PE and backdoor routers will support convergence between the VPN sites. The other routers in the customer sites need only propagate the SoO values carried by the routes, because the routes are forwarded to neighbors. These routers do not otherwise affect or support convergence beyond normal Diffusing Update Algorithm (DUAL) computations.

Router Interoperation with a Site of Origin Extended Community

The configuration of an SoO extended community allows routers that support the EIGRP MPLS VPN PE-CE Site of Origin feature to identify the site from which each route originated. When this feature is enabled, the EIGRP routing process on the PE or CE router checks each received route for the SoO extended community and filters based on the following conditions:

- A received route from BGP or a CE router contains a SoO value that matches the SoO value on the receiving interface.
  
  If a route is received with an associated SoO value that matches the SoO value that is configured on the receiving interface, the route is filtered because it was learned from another PE router or from a backdoor link. This behavior is designed to prevent routing loops.

- A received route from a CE router is configured with an SoO value that does not match.
  
  If a route is received with an associated SoO value that does not match the SoO value that is configured on the receiving interface, the route is added to the EIGRP topology table so that it can be redistributed into BGP.

  If the route is already installed to the EIGRP topology table but is associated with a different SoO value, the SoO value from the topology table will be used when the route is redistributed into BGP.

- A received route from a CE router does not contain an SoO value.
If a route is received without a SoO value, the route is accepted into the EIGRP topology table, and the SoO value from the interface that is used to reach the next hop CE router is appended to the route before it is redistributed into BGP.

When BGP and EIGRP peers that support the SoO extended community receive these routes, they will also receive the associated SoO values and pass them to other BGP and EIGRP peers that support the SoO extended community. This filtering is designed to prevent transient routes from being relearned from the originating site, which prevents transient routing loops from occurring.

Redistribution of BGP VPN Routes That Carry the Site of Origin into EIGRP

When an EIGRP routing process on a PE router redistributes BGP VPN routes into an EIGRP topology table, EIGRP extracts the SoO value (if one is present) from the appended BGP extended community attributes and appends the SoO value to the route before adding it to the EIGRP topology table. EIGRP tests the SoO value for each route before sending updates to CE routers. Routes that are associated with SoO values that match the SoO value configured on the interface are filtered out before they are passed to the CE routers. When an EIGRP routing process receives routes that are associated with different SoO values, the SoO value is passed to the CE router and carried through the CE site.

BGP Cost Community Support for EIGRP MPLS VPN PE-CE Network Topologies

The BGP cost community is a nontransitive extended community attribute that is passed to internal BGP (iBGP) and confederation peers but not external BGP (eBGP) peers. The cost community feature allows you to customize the local route preference and influence the BGP best path selection process.

Before BGP cost community support for EIGRP MPLS VPN PE-CE network topologies was introduced, BGP preferred locally sourced routes over routes learned from BGP peers. Backdoor links in an EIGRP MPLS VPN topology were preferred by BGP when the backdoor link was learned first. (A backdoor link or a route is a connection that is configured outside of the VPN between a remote and main site; for example, a WAN leased line that connects a remote site to the corporate network).

The “prebest path” point of insertion (POI) was introduced in the BGP Cost Community feature to support mixed EIGRP VPN network topologies that contain VPN and backdoor links. This POI is applied automatically to EIGRP routes that are redistributed into BGP. The “prebest path” POI carries the EIGRP route type and metric. This POI influences the best path calculation process by influencing BGP to consider this POI before any other comparison step. No configuration is required. This feature is enabled automatically for EIGRP VPN sites when a Cisco IOS release that supports this feature is installed on the PE routers or the CE and backdoor router at the customer sites.

For more information about the BGP Cost Community feature, see the “BGP Cost Community” module in the Cisco IOS IP Routing: BGP Configuration Guide.

Benefits of the EIGRP MPLS VPN PE-CE Site of Origin Support Feature

The configuration of the EIGRP MPLS VPN PE-CE Site of Origin Support feature introduces per-site VPN filtering, which improves support for complex topologies, such as, MPLS VPNs with backdoor links, CE routers that are dual-homed to different PE routers, and PE routers that support CE routers from different sites within the same virtual routing and forwarding (VRF) instance.
How to Configure EIGRP MPLS VPN PE-CE Site of Origin Support

This section contains the following tasks:

- Configuring the Site of Origin Extended Community, page 5 (required)
- Verifying the Configuration of the SoO Extended Community, page 7 (optional)

Configuring the Site of Origin Extended Community

The configuration of the SoO extended community allows MPLS VPN traffic to be filtered on a per-site basis. The SoO extended community is configured in an inbound BGP route map on the PE router and is applied to the interface. The SoO extended community can be applied to all exit points at the customer site for more specific filtering but must be configured on all interfaces of PE routers that provide VPN services to CE routers.

Prerequisites

- Border Gateway Protocol (BGP) is configured in the network core (or the service provider backbone).
- Configure an EIGRP MPLS VPN before configuring this feature.
- All PE routers that are configured to support the EIGRP MPLS VPN must support the SoO extended community.
- A unique SoO value must be configured for each VPN site. The same value must be used on the interface of the PE router that connects to the CE router for each VPN site.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `route-map map-name {permit | deny} [sequence-number]`
4. `set extcommunity {rt extended-community-value [additive] | soo extended-community-value}
5. `exit`
6. `interface type number`
7. `ip vrf forwarding vrf-name`
8. `ip vrf sitemap route-map-name`
9. `ip address ip-address subnet-mask`
10. `end`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> route-map map-name [permit</td>
<td>Enters route-map configuration mode and creates a route map.</td>
</tr>
<tr>
<td></td>
<td>deny] [sequence-number]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# route-map Site-of-Origin permit 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> set extcommunity rt</td>
<td>Sets BGP extended community attributes.</td>
</tr>
<tr>
<td></td>
<td>extended-community-value [additive]</td>
</tr>
<tr>
<td></td>
<td>soo extended-community-value</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-route-map)# set extcommunity soo 100:1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits route-map configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-route-map)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> interface type number</td>
<td>Enters interface configuration mode to configure the specified interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface FastEthernet 0/0</td>
<td></td>
</tr>
</tbody>
</table>
### What to Do Next

- To verify the configuration of the SoO extended community, follow the steps in the next section, “Verifying the Configuration of the SoO Extended Community.”
- For mixed EIGRP MPLS VPN network topologies that contain backdoor routes, the next task is to configure the “prebest path” cost community for backdoor routes.

### Verifying the Configuration of the SoO Extended Community

Use the following steps to verify the configuration of the SoO extended community attribute.

#### SUMMARY STEPS

1. **enable**
2. `show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [ip-prefix/length [longer-prefixes] [output-modifiers]] [network-address [mask] [longer-prefixes] [output-modifiers]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [tags]`
3. `show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] topology [topology-name] [ip-address] [active] [all-links] [detail-links] [pending] [summary] [zero-successors] [route-type {connected | external | internal | local | redistributed | summary | vpn}]`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> ip vrf forwarding vrf-name</td>
<td>Associates the VRF with an interface or subinterface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# ip vrf forwarding VRF1</code></td>
<td>• The VRF name configured in this step should match the VRF name created for the EIGRP MPLS VPN with the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature.</td>
</tr>
<tr>
<td><strong>Step 8</strong> ip vrf sitemap route-map-name</td>
<td>Associates the VRF with an interface or subinterface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# ip vrf sitemap Site-of-Origin</code></td>
<td>• The route map name configured in this step should match the route map name created to apply the SoO extended community in Step 3.</td>
</tr>
<tr>
<td><strong>Step 9</strong> ip address ip-address subnet-mask</td>
<td>Configures the IP address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# ip address 10.0.0.1 255.255.255.255</code></td>
<td>• The IP address needs to be reconfigured after enabling VRF forwarding.</td>
</tr>
<tr>
<td><strong>Step 10</strong> end</td>
<td>Exits interface configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show ip bgp vpnv4</td>
<td>Displays VPN address information from the BGP table.</td>
</tr>
<tr>
<td>all rd {route-distinguisher} vrf vrf-name ip-prefix</td>
<td>- Use the show ip bgp vpnv4 command with the all keyword to verify that the specified route has been configured with the SoO extended community attribute.</td>
</tr>
<tr>
<td>Example: Router# show ip bgp vpnv4 all 10.0.0.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show eigrp address-family</td>
<td>Displays entries in the EIGRP topology table.</td>
</tr>
<tr>
<td>{ipv4</td>
<td>ipv6} vrf vrf-name</td>
</tr>
<tr>
<td>multicast topology topology-name</td>
<td>- ip-address [active] all-links</td>
</tr>
<tr>
<td>detail-links pending summary</td>
<td>- zero-successors route-type {connected external internal local redistributed summary vpn}</td>
</tr>
<tr>
<td>Example: Router# show eigrp address-family ipv4 4453 topology 10.10.10.0/24</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Examples for EIGRP MPLS VPN PE-CE SoO

This section contains the following configuration examples:

- Configuring the Site of Origin Extended Community: Example, page 8
- Verifying the Site of Origin Extended Community: Examples, page 9

Configuring the Site of Origin Extended Community: Example

The following example, beginning in global configuration mode, configures the SoO extended community on an interface:

Router(config)# route-map Site-of-Origin permit 10
Router(config-route-map)# set extcommunity soo 100:1
Router(config-route-map)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip vrf forwarding VRP1
Router(config-if)# ip vrf sitemap Site-of-Origin
Router(config-if)# ip address 10.0.0.1 255.255.255.255
Router(config-if)# end
Verifying the Site of Origin Extended Community: Examples

The following example shows VPN address information from the BGP table and verifies the configuration of the SoO extended community:

```
Router# show ip bgp vpnv4 all 10.0.0.1
```

BGP routing table entry for 100:1:10.0.0.1/32, version 6
Paths: (1 available, best #1, no table)
  Advertised to update-groups:
    1
    100 300
    192.168.0.2 from 192.168.0.2 (172.16.13.13)
  Origin incomplete, localpref 100, valid, external, best
  Extended Community: S0O:100:1

The following example shows how to display EIGRP metrics for specified internal services and external services:

```
Router# show eigrp address-family ipv4 4453 topology 10.10.10.0/24
```

EIGRP-IPv4 VR(virtual-name) Topology Entry for AS(4453)/ID(10.0.0.1) for 10.10.10.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 128256
Descriptor Blocks:
  0.0.0.0 (Null0), from Connected, Send flag is 0x0
  Composite metric is (128256/0), service is Internal
Vector metric:
  Minimum bandwidth is 10000000 Kbit
  Total delay is 5000 microseconds
  Reliability is 255/255
  Load is 1/255
  Minimum MTU is 1514
  Hop count is 0
  Originating router is 10.0.0.1

Additional References

The following sections provide references related to the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP cost community feature and the “prebest path” point of insertion</td>
<td>BGP Cost Community</td>
</tr>
<tr>
<td>Cisco Express Forwarding (CEF) commands</td>
<td>Cisco IOS IP Switching Command Reference</td>
</tr>
<tr>
<td>CEF configuration tasks</td>
<td>Cisco Express Forwarding Overview</td>
</tr>
<tr>
<td>EIGRP commands</td>
<td>Cisco IOS IP Routing Protocols: EIGRP Command Reference</td>
</tr>
<tr>
<td>EIGRP configuration tasks</td>
<td>Configuring EIGRP</td>
</tr>
<tr>
<td>MPLS VPNs</td>
<td>MPLS Layer 3 VPN Features Roadmap</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Feature Information for MPLS VPN PE-CE Site of Origin (SoO)

Table 1 lists the release history for this feature.

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

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

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

Table 1 Feature Information for EIGRP MPLS VPN PE-CE Site of Origin (SoO)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP MPLS VPN PE-CE Site of Origin (SoO)</td>
<td>12.0(27)S</td>
<td>The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces the capability to filter MPLS VPN traffic on a per-site basis for EIGRP networks.</td>
</tr>
<tr>
<td></td>
<td>12.3(8)T</td>
<td>The following command was introduced or modified by this feature: ip vrf sitemap</td>
</tr>
<tr>
<td></td>
<td>12.2(18)SXE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(28)SB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(30)S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15.0(1)M</td>
<td></td>
</tr>
</tbody>
</table>
Glossary

AFI—Address Family Identifier. Carries the identity of the network layer protocol that is associated with the network address.

backdoor router—A router that connects two or more sites, that are also connected to each other through an MPLS VPN EIGRP PE to CE links.

backdoor link—A link connecting two backdoor routers.

BGP—Border Gateway Protocol. An interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined by RFC 1163, *A Border Gateway Protocol (BGP)*. BGP supports CIDR and uses route aggregation mechanisms to reduce the size of routing tables.

Cost Community—An extended community attribute that can be inserted anywhere into the best path calculation.

customer edge (CE) router—A router that belongs to a customer network, that connects to a provider edge (PE) router to utilize MPLS VPN network services.

MBGP—multiprotocol BGP. An enhanced version of BGP that carries routing information for multiple network-layer protocols and IP multicast routes. It is defined in RFC 2858, *Multiprotocol Extensions for BGP-4*.

provider edge (PE) router—The PE router is the entry point into the service provider network. The PE router is typically deployed on the edge of the network and is administered by the service provider. The PE router is the redistribution point between EIGRP and BGP in PE to CE networking.

site—A collection of routers that have well-defined exit points to other “sites.”

site of origin (SoO)—A special purpose tag or attribute that identifies the site that injects a route into the network. This attribute is used for intersite filtering in MPLS VPN PE-to-CE topologies.

VPN—Virtual Private Network. Allows IP traffic to travel securely over public TCP/IP networks and the Internet by encapsulating and encrypting all IP packets. VPN uses a tunnel to encrypt all information at the IP level.

© 2004–2009 Cisco Systems, Inc. All rights reserved.
EIGRP MIB

First Published: February 28, 2005
Last Updated: October 2, 2009

The EIGRP MIB feature introduces an Enhanced Interior Gateway Routing Protocol (EIGRP) MIB in Cisco IOS software. This MIB is accessed through remote Simple Network Management Support (SNMP) software clients. This MIB provides full EIGRP support for GET requests and limited notification (TRAP) support for stuck-in-active (SIA) and neighbor authentication failure events.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for EIGRP MIB” section on page 12.

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

Contents

- Prerequisites for EIGRP MIB, page 2
- Restrictions for EIGRP MIB, page 2
- Information About EIGRP MIB, page 2
- How to Enable EIGRP MIB, page 8
- Configuration Examples for Enabling EIGRP MIB, page 9
- Additional References, page 10
- Feature Information for EIGRP MIB, page 12
Prerequisites for EIGRP MIB

- EIGRP MIB table objects are not visible via SNMP until an EIGRP routing process is enabled and an SNMP community string is configured on at least one router.
- Support for EIGRP notifications (TRAP) is not activated until a trap destination is configured.

Restrictions for EIGRP MIB

- EIGRP MIB support has not been implemented for the EIGRP Prefix Limit Support feature.
- EIGRP MIB support is available for IPv4 only.

Information About EIGRP MIB

The following concepts relate to EIGRP MIB:
- EIGRP MIB Overview, page 2
- EIGRP VPN Table, page 2
- EIGRP Traffic Statistics Table, page 3
- EIGRP Topology Table, page 4
- EIGRP Neighbor Table, page 5
- EIGRP Interface Table, page 6
- EIGRP Notifications, page 7

EIGRP MIB Overview

The EIGRP MIB feature introduces EIGRP MIB support in Cisco IOS software. EIGRP routing processes that run over IPv4 are supported. The EIGRP MIB is accessed through remote SNMP software clients. MIB table objects are accessed as read-only through GET, GETINFO, GETMANY, GETNEXT, GETBULK, and SET requests. Counters for MIB table objects are cleared when the EIGRP routing process is reset or when the routing table is refreshed by entering the clear ip route or clear ip eigrp commands, or by entering clear eigrp address-family commands. Managed objects for all EIGRP routing processes are implemented as five table objects on a per-autonomous-system or per-Virtual-Private-Network (VPN) basis.

EIGRP VPN Table

The EIGRP VPN Table contains information regarding which VPNs are configured to run an EIGRP routing process. VPN routes are indexed by the VPN name and the EIGRP autonomous system number. The EIGRP VPN table object and the value populated for that object are described in Table 1.
The EIGRP Traffic Statistics Table contains counters and statistics for the specific types of EIGRP packets that are sent and the related collective information that is generated. The objects in this table are populated on a per-autonomous-system basis. Objects in this table are populated for adjacencies formed on all interfaces with an IP address that is configured under an EIGRP network statement. Traffic statistics table objects and the values populated for each object are described in Table 2.

Table 1  VPN Table Object Description

<table>
<thead>
<tr>
<th>EIGRP VPN Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cEigrpVpnName</td>
<td>The VPN routing and forwarding (VRF) name. Only VRFs that are configured to run an EIGRP routing process are populated.</td>
</tr>
</tbody>
</table>

Table 2  Traffic Statistics Table Object Descriptions

<table>
<thead>
<tr>
<th>EIGRP Traffic Statistics Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cEigrpNbrCount</td>
<td>Total number of live neighbors. This table object is incremented or decremented as peering sessions are established or expired.</td>
</tr>
<tr>
<td>cEigrpHellosSent</td>
<td>Total number of transmitted hello packets. This table object is incremented as packets are transmitted.</td>
</tr>
<tr>
<td>cEigrpHellosRcvd</td>
<td>Total number of received hello packets. This table object is incremented as packets are received.</td>
</tr>
<tr>
<td>cEigrpUpdatesSent</td>
<td>Total number of transmitted routing update packets. This table object is incremented as packets are transmitted.</td>
</tr>
<tr>
<td>cEigrpUpdatesRcvd</td>
<td>Total number of received routing update packets. This table object is incremented as packets are received.</td>
</tr>
<tr>
<td>cEigrpQueriesSent</td>
<td>Total number of alternate route query packets transmitted. This table object is incremented as packets are transmitted.</td>
</tr>
<tr>
<td>cEigrpQueriesRcvd</td>
<td>Total number of alternate route query packets received. This table object is incremented as packets are received.</td>
</tr>
<tr>
<td>cEigrpRepliesSent</td>
<td>Total number of reply packets that are transmitted in response to received query packets. This table object is incremented as packets are transmitted.</td>
</tr>
<tr>
<td>cEigrpRepliesRcvd</td>
<td>Total number of reply packets that are received in response to transmitted query packets. This table object is incremented as packets are transmitted.</td>
</tr>
<tr>
<td>cEigrpAcksSent</td>
<td>Total number of acknowledgment packets that are transmitted in response to received update packets. This table object is incremented as packets are transmitted.</td>
</tr>
<tr>
<td>cEigrpAcksRcvd</td>
<td>Total number of acknowledgment packets that are received in response to transmitted update packets. This table object is incremented as packets are received.</td>
</tr>
<tr>
<td>cEigrpInputQHighMark</td>
<td>The highest number of packets that have been in the input queue. This table object is incremented only when the previous highest number is exceeded.</td>
</tr>
</tbody>
</table>
EIGRP Topology Table

The EIGRP Topology Table contains information regarding EIGRP routes received in updates and routes that are locally originated. EIGRP sends routing updates to and receives routing updates from adjacent routers to which peering relationships (adjacencies) have been formed. The objects in this table are populated on a per-topology-table-entry (route) basis. Topology table objects and the values populated for each object are described in Table 3.

Table 3  Topology Table Object Descriptions

<table>
<thead>
<tr>
<th>EIGRP Topology Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cEigrpActive</td>
<td>Displays the active status for routes in the topology table. The value for this table object is displayed on a per-route basis. A value of 1 is displayed when a route has gone into an active state. A value of 2 is displayed when a route is in a passive state (normal).</td>
</tr>
<tr>
<td>cEigrpStuckInActive</td>
<td>Displays the SIA status of a route. The value for this table object is displayed on a per-route basis. A value of 1 is displayed when a route is in an SIA state (no reply has been received for queries for alternate paths). SIA queries are transmitted when a route is placed in this state.</td>
</tr>
</tbody>
</table>
Table 3  Topology Table Object Descriptions (continued)

<table>
<thead>
<tr>
<th>Object Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cEigrpDestSuccessors</strong></td>
</tr>
<tr>
<td>Total number successors (a route that is the next hop to a destination network)</td>
</tr>
<tr>
<td>for a topology table entry. The topology table will contain a successor for each</td>
</tr>
<tr>
<td>path to a given destination. This table object is incremented each time a</td>
</tr>
<tr>
<td>successor is added or removed.</td>
</tr>
<tr>
<td><strong>cEigrpFdistance</strong></td>
</tr>
<tr>
<td>The feasible (best) distance to a destination network. This value is used to</td>
</tr>
<tr>
<td>calculate the feasible successor for a topology table entry.</td>
</tr>
<tr>
<td><strong>cEigrpRouteOriginAddr</strong></td>
</tr>
<tr>
<td>The protocol type of an IP address defined in the origin of the topology table</td>
</tr>
<tr>
<td>entry.</td>
</tr>
<tr>
<td><strong>cEigrpRouteOriginType</strong></td>
</tr>
<tr>
<td>Displays the IP address of the router that originated the route in the topology</td>
</tr>
<tr>
<td>table entry. The table is populated only if the topology table entry was not</td>
</tr>
<tr>
<td>locally originated.</td>
</tr>
<tr>
<td><strong>cEigrpNextHopAddress</strong></td>
</tr>
<tr>
<td>Displays the protocol type for the next-hop IP address for the route in a</td>
</tr>
<tr>
<td>topology table entry.</td>
</tr>
<tr>
<td><strong>cEigrpNextHopAddress</strong></td>
</tr>
<tr>
<td>The next-hop IP address for a route in a topology table entry.</td>
</tr>
<tr>
<td><strong>cEigrpNextHopInterface</strong></td>
</tr>
<tr>
<td>The interface through which the next-hop IP address is reached to send traffic</td>
</tr>
<tr>
<td>to the destination.</td>
</tr>
<tr>
<td><strong>cEigrpDistance</strong></td>
</tr>
<tr>
<td>The computed distance to the destination network entry from the local router.</td>
</tr>
<tr>
<td><strong>cEigrpReportDistance</strong></td>
</tr>
<tr>
<td>The computed distance to the destination network in the topology entry as</td>
</tr>
<tr>
<td>reported by the originator of the route.</td>
</tr>
</tbody>
</table>

**Table 3**  Topology Table Object Descriptions (continued)

EIGRP Neighbor Table

The EIGRP Neighbor Table contains information about EIGRP neighbors to which adjacencies have been established. EIGRP uses a “Hello” protocol to form neighbor relationships with directly connected EIGRP neighbors. The objects in this table are populated on a per-neighbor basis. Neighbor table objects and the values populated for each object are described in Table 4.

Table 4  Neighbor Table Object Descriptions

<table>
<thead>
<tr>
<th>EIGRP Neighbor Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cEigrpPeerAddrType</strong></td>
<td>The protocol type of the remote source IP address used by the neighbor to</td>
</tr>
<tr>
<td></td>
<td>establish the EIGRP adjacency with the local router.</td>
</tr>
<tr>
<td><strong>cEigrpPeerAddr</strong></td>
<td>The source IP address of the neighbor that was used to establish EIGRP</td>
</tr>
<tr>
<td></td>
<td>adjacency with the local router.</td>
</tr>
<tr>
<td><strong>cEigrpPeerInterface</strong></td>
<td>The name of the local interface, through which the neighbor can be reached.</td>
</tr>
<tr>
<td></td>
<td>This table object is populated on a per-neighbor basis.</td>
</tr>
<tr>
<td><strong>cEigrpPeerIfIndex</strong></td>
<td>The index of the local interface, through which this neighbor can be</td>
</tr>
<tr>
<td></td>
<td>reached.</td>
</tr>
<tr>
<td><strong>cEigrpHoldTime</strong></td>
<td>The hold timer value for the adjacency with the neighbor. If this timer</td>
</tr>
<tr>
<td></td>
<td>expires, the neighbor is declared down and removed from the neighbor table.</td>
</tr>
<tr>
<td><strong>cEigrpUpTime</strong></td>
<td>The length of time for which the EIGRP adjacency to the neighbor has been</td>
</tr>
<tr>
<td></td>
<td>in an up state. The time period is displayed in hours:minutes:seconds.</td>
</tr>
</tbody>
</table>
EIGRP Interface Table

The EIGRP Interface Table contains information and statistics for each interface that EIGRP has been configured to run over. The objects in this table are populated on a per-interface basis. Interface table objects and the values populated for each object are described in Table 5.

<table>
<thead>
<tr>
<th>Table 5</th>
<th>EIGRP Interface Table Object Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP Interface Table</td>
<td>Description</td>
</tr>
<tr>
<td>cEigrpPeerCount</td>
<td>Total number of neighbor adjacencies formed through this interface.</td>
</tr>
<tr>
<td>cEigrpXmitReliableQ</td>
<td>Total number of packets waiting in the reliable transport transmission queue (acknowledgment is required) to be sent to a neighbor.</td>
</tr>
<tr>
<td>cEigrpXmitUnreliableQ</td>
<td>Total number of packets waiting in the unreliable transmission queue (no acknowledgment required).</td>
</tr>
<tr>
<td>cEigrpMeanSrtt</td>
<td>The computed SRTT for packets transmitted to and received from all neighbors on the interface.</td>
</tr>
<tr>
<td>cEigrpPacingReliable</td>
<td>The configured time interval (in milliseconds) between EIGRP packet transmissions on this interface when the reliable transport is used.</td>
</tr>
<tr>
<td>cEigrpPacingUnreliable</td>
<td>The configured time interval (in milliseconds) between EIGRP packet transmissions on this interface when the unreliable transport is used.</td>
</tr>
<tr>
<td>cEigrpMFlowTimer</td>
<td>The configured multicast flow control timer value (in milliseconds) for this interface.</td>
</tr>
<tr>
<td>cEigrpPendingRoutes</td>
<td>Total number of routing updates queued for transmission on this interface.</td>
</tr>
</tbody>
</table>
EIGRP MIB

Information About EIGRP MIB

EIGRP Notifications

The EIGRP MIB provides limited notification (TRAP) support for SIA and neighbor authentication failure events. The `snmp-server enable traps eigrp` command is used to enable EIGRP notifications on a Cisco router. Support for TRAP events is not activated until a trap destination is configured with the `snmp-server host` command and a community string is defined with the `snmp-server community` command. EIGRP notifications are described in Table 6.

<table>
<thead>
<tr>
<th>ObjectName</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cEigrpHelloInterval</td>
<td>The configured time interval (in seconds) between Hello packet transmissions for this interface.</td>
</tr>
<tr>
<td>cEigrpXmitNextSerial</td>
<td>The serial number of the next packet that is queued for transmission on this interface.</td>
</tr>
<tr>
<td>cEigrpUMcasts</td>
<td>Total number of unreliable (no acknowledgment required) multicast packets transmitted on this interface.</td>
</tr>
<tr>
<td>cEigrpRMcasts</td>
<td>Total number of reliable (acknowledgment required) multicast packets transmitted on this interface.</td>
</tr>
<tr>
<td>cEigrpUUcasts</td>
<td>Total number of unreliable (no acknowledgment required) unicast packets transmitted on this interface.</td>
</tr>
<tr>
<td>cEigrpRUcasts</td>
<td>Total number of reliable (acknowledgment required) unicast packets transmitted on this interface.</td>
</tr>
<tr>
<td>cEigrpMcastExcept</td>
<td>The total number of EIGRP multicast exception transmissions that have occurred on this interface.</td>
</tr>
<tr>
<td>cEigrpCRpkts</td>
<td>Total number conditional-receive packets sent on this interface.</td>
</tr>
<tr>
<td>cEigrpAcksSuppressed</td>
<td>Total number of individual acknowledgment packets that have been suppressed and combined in an already enqueued outbound reliable packet on this interface.</td>
</tr>
<tr>
<td>cEigrpRetranSent</td>
<td>Total number of packet retransmissions sent on this interface.</td>
</tr>
<tr>
<td>cEigrpOOSrvcd</td>
<td>Total number of out-of-sequence packets received on this interface.</td>
</tr>
<tr>
<td>cEigrpAuthMode</td>
<td>The authentication mode configured for traffic that uses this interface. The value of 0 is displayed when no authentication is enabled. The value of 1 is displayed when message digest algorithm 5 (MD5) authentication is enabled.</td>
</tr>
<tr>
<td>cEigrpAuthKeyChain</td>
<td>The name of the authentication key chain configured on this interface. The key chain is a reference to which set of secret keys is to be accessed to determine which key string to use. The key-chain name is not the key string (password).</td>
</tr>
</tbody>
</table>
Table 6  EIGRP Notifications

<table>
<thead>
<tr>
<th>EIGRP Traps (Notifications)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cEigrpAuthFailureEvent</td>
<td>When EIGRP MD5 authentication is enabled on any interface and neighbor adjacencies are formed, a notification is sent if any adjacency goes down as a result of an authentication failure. This notification will be sent once per down event. This notification includes the source IP address of the neighbor from which the authentication failure occurred.</td>
</tr>
<tr>
<td>cEigrpRouteStuckInActive</td>
<td>During the query phase for a new route to a destination network, the route is placed in the active state (an alternate path is actively being sought) and a query packet is broadcast to the network. If no replies are received to the query, an SIA query packets are broadcast. If a reply is not received for the SIA queries, the neighbor adjacency is dropped, the route is declared SIA, and this notification is sent.</td>
</tr>
</tbody>
</table>

How to Enable EIGRP MIB

This section contains the following task:

- Enabling EIGRP MIB, page 8 (required)

Enabling EIGRP MIB

Perform this task to enable an EIGRP MIB. This task specifies an SNMP server host, configures an SNMP community access string, and enables EIGRP notifications.

SUMMARY STEPS

1. enable
2. configure terminal
3. snmp-server host { [hostname | ip-address] | [vrf vrf-name] | [traps | informs] | [version {1 | 2c | 3} | [auth | noauth | priv]] | community-string | [udp-port port] | [notification-type] | [vrrp] } [ipv6 nacl] [access-list-number]
4. snmp-server community string [view view-name] [ro | rw | [ipv6 nacl] [access-list-number]
5. snmp-server enable traps eigrp
6. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server host</td>
<td>Specifies the destination host or address for SNMP notifications.</td>
</tr>
<tr>
<td>hostname</td>
<td>ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> snmp-server community string view view-name</td>
<td>Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.</td>
</tr>
<tr>
<td>[ro</td>
<td>rw]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# snmp-server community EIGRP1NET1A</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> snmp-server enable traps eigrp</td>
<td>Enables SNMP support for EIGRP notifications.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Notifications can be configured for only SIA and neighbor authentication failure events.</td>
</tr>
<tr>
<td>Router(config)# snmp-server enable traps eigrp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuration Examples for Enabling EIGRP MIB

The following examples show how to configure and verify this feature:

- **EIGRP MIB Configuration: Example, page 10**
- **EIGRP MIB Verification: Example, page 10**
EIGRP MIB Configuration: Example

In the following example, an SNMP server host is specified, a community string is configured, and support for EIGRP notifications is enabled:

```
Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp
Router(config)# snmp-server community EIGRP1NET1A
Router(config)# snmp-server enable traps eigrp
```

EIGRP MIB Verification: Example

In the following example, the local SNMP configuration is verified by entering the `show running-config` command:

```
Router# show running-config | include snmp

snmp-server community EIGRP1NET1A
snmp-server enable traps eigrp
snmp-server host 10.0.0.1 version 2c NETMANAGER
```

Additional References

The following sections provide references related to the EIGRP MIB feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP commands</td>
<td>Cisco IOS IP Routing: EIGRP Command Reference</td>
</tr>
<tr>
<td>Basic EIGRP configuration tasks</td>
<td>“Configuring EIGRP” module</td>
</tr>
<tr>
<td>Troubleshooting SIA events</td>
<td>What Does the EIGRP DUAL-3-SIA Error Message Mean?</td>
</tr>
<tr>
<td>SNMP commands</td>
<td>Cisco IOS Network Management Command Reference</td>
</tr>
<tr>
<td>SNMP configuration tasks</td>
<td>“Configuring SNMP Support” module</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-EIGRP-MIB.my</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC-1213</td>
<td>Management Information Base for Network Management of TCP/IP-based Internets: MIB-II</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Feature Information for EIGRP MIB

Table 7 lists the release history for this feature.

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

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

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP MIB</td>
<td>12.3(14)T</td>
<td>The EIGRP MIB feature introduces an EIGRP MIB in Cisco IOS software. This MIB is accessed through remote Simple Network Management Support (SNMP) software clients. This MIB provides full EIGRP support for GET requests and limited notification (TRAP) support for stuck-in-active (SIA) and neighbor authentication failure events. The following commands were new or modified for this release: <code>snmp-server enable traps eigrp</code>, <code>snmp-server host</code>.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15.0(1)M</td>
<td></td>
</tr>
</tbody>
</table>

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.
EIGRP Prefix Limit Support

First Published: August 9, 2004
Last Updated: October 2, 2009

The EIGRP Prefix Limit Support feature introduces the capability to limit the number of prefixes per VRF that are accepted from a specific peer or to limit all prefixes that are accepted by an Enhanced Interior Gateway Routing Protocol (EIGRP) process through peering and redistribution. This feature is designed to protect the local router from external misconfiguration that can negatively impact local system resources; for example, a peer that is misconfigured to redistribute full Border Gateway Protocol (BGP) routing tables into EIGRP. This feature is enabled under the IPv4 VRF address family and can be configured to support the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature.

For more information about EIGRP MPLS VPN configuration, refer to the “EIGRP MPLS VPN PE-CE Site of Origin (SoO)” module.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for EIGRP Prefix Limit Support” section on page 22.

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

Contents

- Prerequisites for EIGRP Prefix Limit Support, page 2
- Restrictions for EIGRP Prefix Limit Support, page 2
- Information About EIGRP Prefix Limit Support, page 2
- How to Configure the Maximum-Prefix Limit, page 4
Prerequisites for EIGRP Prefix Limit Support

- Multi Protocol Label Switching (MPLS) Virtual Private Network (VPN) services have been configured between the Provider Edge (PE) routers and the customer edge (CE) routers at the customer sites.

Restrictions for EIGRP Prefix Limit Support

- This feature is supported only under the IPv4 VRF address family and can be used only to limit the number of prefixes that are accepted through a VRF.
- The EIGRP Prefix Limiting Support feature is enabled only under the IPv4 VRF address-family. A peer that is configured to send too many prefixes or a peer that rapidly advertises and then withdraws prefixes can cause instability in the network. This feature can be configured to automatically reestablish a disabled peering session at the default or user-defined time interval or when the maximum-prefix limit is not exceeded. However, the configuration of this feature alone cannot change or correct a peer that is sending an excessive number of prefixes. If the maximum-prefix limit is exceeded, you will need to reconfigure the maximum-prefix limit or reduce the number of prefixes that are sent from the peer.

Information About EIGRP Prefix Limit Support

To configure the EIGRP Prefix Limit Support feature, you must understand the following concepts:

- Misconfigured VPN Peers, page 2
- EIGRP Prefix Limit Support Overview, page 3
- Warning-Only Mode, page 3
- Restart, Reset, and Dampening Timers and Counters, page 4

Misconfigured VPN Peers

In MPLS VPNs, the number of routes that are permitted in the VPN routing and forwarding instance (VRF) is configured with the maximum routes VRF configuration command. However, limiting the number routes permitted in the VPN does not protect the local router from a misconfigured peer that sends an excessive number of routes or prefixes. This type of external misconfiguration can have a negative effect on the local router by consuming all available system resources (CPU and memory) in processing prefix updates. This type of misconfiguration can occur on a peer that is not within the control of the local administrator.
EIGRP Prefix Limit Support Overview

The EIGRP Prefix Limit Support feature provides the ability to configure a limit on the number of prefixes that are accepted from EIGRP peers or learned through redistribution. This feature can be configured on per-peer or per-process basis and can be configured for all peers and processes. This feature is designed to protect the local router from misconfigured external peers by limiting the amount of system resources that can be consumed to process prefix updates.

Protecting the Router from External Peers

This feature can be configured to protect an individual peering session or protect all peering sessions. When this feature is enabled and the maximum-prefix limit has been exceeded, the router will tear down the peering session, clear all routes that were learned from the peer, and then place the peer in a penalty state for the default or user-defined time period. After the penalty time period expires, normal peering will be reestablished.

Limiting the Number of Redistributed Prefixes

This feature can be configured to limit the number of prefixes that are accepted into the EIGRP topology table through redistribution from the Routing Information Base (RIB). All sources of redistribution are processed cumulatively. When the maximum-prefix limit is exceeded, all routes learned through redistribution are discarded and redistribution is suspended for the default or user-defined time period. After the penalty time period expires, normal redistribution will occur.

Protecting the Router at the EIGRP Process Level

This feature can be configured to protect the router at the EIGRP process level. When this feature is configured at the EIGRP process level, the maximum-prefix limit is applied to all peering sessions and to route redistribution. When the maximum-prefix limit is exceeded, all sessions with the remote peers are torn down, all routes learned from remote peers are removed from the topology and routing tables, all routes learned through redistribution are discarded, and redistribution and peering are suspended for the default or user-defined time period.

Warning-Only Mode

The EIGRP Prefix Limit Support feature has two modes of operation. This feature can control peering and redistribution per default and user-defined values or this feature can operate in warning-only mode. In warning-only mode the router will monitor the number of prefixes learned through peering and/or redistribution but will not take any action when the maximum-prefix limit is exceeded. Warning-only mode is activated only when the warning-only keyword is configured for any of the maximum-prefix limit commands. Only syslog messages are generated when this mode of operation is enabled. Syslog messages can be sent to a syslog server or printed in the console. These messages can be buffered or rate limited per standard Cisco IOS system logging configuration options. For more information about system logging in Cisco IOS software, refer to the “Troubleshooting and Fault Management” module.
Restart, Reset, and Dampening Timers and Counters

The EIGRP Prefix Limit Support feature provides two user-configurable timers, a restart counter, and a dampening mechanism. When the maximum-prefix limit is exceeded, peering and/or redistribution is suspended for a default or user-defined time period. If the maximum-prefix limit is exceeded too often, redistribution and/or peering will be suspended until manual intervention is taken.

Restart Timer

The restart timer determines how long the router will wait to form an adjacency or accept redistributed routes from the RIB after the maximum-prefix limit has been exceeded. The default restart-time period is 5 minutes.

Restart Counter

The restart counter determines the number of times a peering session can be automatically reestablished after the peering session has been torn down or after the redistributed routes have been cleared and relearned because the maximum-prefix limit has been exceeded. The default restart-count limit is three.

Caution

After the restart count limit has been crossed, you will need to enter the `clear ip route *`, `clear ip eigrp neighbor`, or `clear eigrp address-family neighbor` command to restore normal peering and redistribution.

Reset Timer

The reset timer is used to configure the router to reset the restart count to 0 after the default or configured reset-time period has expired. This timer is designed to provide administrator with control over long-and medium-term accumulated penalties. The default reset-time period is 15 minutes.

Dampening Mechanism

The dampening mechanism is used to apply an exponential decay penalty to the restart-time period each time the maximum-prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart-time value in minutes. This mechanism is designed to identify and suppress unstable peers. It is disabled by default.

How to Configure the Maximum-Prefix Limit

This section contains the following tasks:

- Configuring the Maximum Number of Prefix Accepted from Peering Sessions: Autonomous System Configuration, page 5 (required)
- Configuring the Maximum Number of Prefixes Accepted from Peering Sessions: Named Configuration, page 7 (required)
- Configuring the Maximum Number of Prefixes Learned Through Redistribution: Autonomous System Configuration, page 9 (required)
Configuring the Maximum Number of Prefix Accepted from Peering Sessions: Autonomous System Configuration

The maximum-prefix limit can be configured for all peering sessions or individual peering sessions with the `neighbor maximum-prefix` (EIGRP) command. When the maximum-prefix limit is exceeded, the session with the remote peer is torn down and all routes learned from the remote peer are removed from the topology and routing tables. The maximum-prefix limit that can be configured is limited only by the available system resources on the router.

Note

In EIGRP, `neighbor` commands have been used traditionally to configure static neighbors. In the context of this feature, however, the `neighbor maximum-prefix` command can be used to configure the maximum-prefix limit for both statically configured and dynamically discovered neighbors.

Inherited Timer Values

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the `maximum-prefix` command, are inherited by the `redistribute maximum-prefix` and `neighbor maximum-prefix` command configurations by default. If a single peer is configured with the `neighbor maximum-prefix` command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

Prerequisites

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

Restrictions

- This task can be configured only in IPv4 VRF address family configuration mode.
- When you configure the `neighbor maximum-prefix` command to protect a single peering session, only the maximum-prefix limit, the percentage threshold, the warning-only configuration options can be configured. Session dampening, restart, and reset timers are configured on a global basis.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router eigrp as-number`
### How to Configure the Maximum-Prefix Limit

1. **address-family ipv4 [unicast] vrf vrf-name**
2. **neighbor {ip-address | peer-group-name} description text**
3. **neighbor ip-address maximum-prefix maximum [threshold] [warning-only]**
4. **neighbor maximum-prefix maximum [threshold] [dampened] [reset-time minutes] [restart minutes] [restart-count number] [warning-only]**

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router eigrp as-number</td>
<td>Enters router configuration mode and creates an EIGRP routing process.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# router eigrp 1</td>
<td>• A maximum of 30 EIGRP routing processes can be configured.</td>
</tr>
<tr>
<td><strong>Step 4</strong> address-family ipv4 [unicast] vrf vrf-name</td>
<td>Enters address family configuration mode and creates a session for the VRF.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router)# address-family ipv4 vrf vrf1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> neighbor (ip-address</td>
<td>peer-group-name) description text</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af)# neighbor 172.16.2.3 description peer with example.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> neighbor ip-address maximum-prefix maximum [threshold] [warning-only]</td>
<td>Limits the number of prefixes that are accepted from the specified EIGRP neighbor.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 10000 80 warning-only</td>
<td></td>
</tr>
</tbody>
</table>
### Troubleshooting Tips

If an individual peer or all peers have exceeded the maximum-prefix limit the same number of times as the default or user-defined restart-count value, the individual session or all sessions will need to be manually reset with the `clear ip route` or `clear ip eigrp neighbor` command before normal peering can be reestablished.

### Configuring the Maximum Number of Prefixes Accepted from Peering Sessions: Named Configuration

The maximum-prefix limit can be configured for all peering sessions or individual peering sessions with the `neighbor maximum-prefix` (EIGRP) command. When the maximum-prefix limit is exceeded, the session with the remote peer is torn down and all routes learned from the remote peer are removed from the topology and routing tables. The maximum-prefix limit that can be configured is limited only by the available system resources on the router.

#### Note

In EIGRP, `neighbor` commands have been used traditionally to configure static neighbors. In the context of this feature, however, the `neighbor maximum-prefix` command can be used to configure the maximum-prefix limit for both statically configured and dynamically discovered neighbors.

### Inherited Timer Values

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the `maximum-prefix` command, are inherited by the `redistribute maximum-prefix` and `neighbor maximum-prefix` command configurations by default. If a single peer is configured with the `neighbor maximum-prefix` command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

### Prerequisites

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.
Restrictions

- This task can be configured only in IPv4 VRF address family configuration mode.
- When you configure the `neighbor maximum-prefix` command to protect a single peering session, only the maximum-prefix limit, the percentage threshold, and the warning-only configuration options can be configured. Session dampening, restart, and reset timers are configured on a global basis.

SUMMARY STEPS

1. enable
2. configure terminal
3. router eigrp virtual-instance-name
4. address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number
5. neighbor ip-address | peer-group-name description text
6. neighbor ip-address maximum-prefix maximum [threshold] [warning-only]
7. neighbor maximum-prefix maximum [threshold] [dampened] [reset-time minutes] [restart minutes] [restart-count number] [warning-only]
8. exit-address-family

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 router eigrp virtual-instance-name</td>
<td>Enters router configuration mode and creates an EIGRP routing process.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# router eigrp virtual-name</td>
<td>A maximum of 30 EIGRP routing processes can be configured.</td>
</tr>
<tr>
<td>Step 4 address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
<td>Enters address family configuration mode and creates a session for the VRF.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-router)# address-family ipv4 vrf RED autonomous-system 45000</td>
<td></td>
</tr>
</tbody>
</table>
EIGRP Prefix Limit Support

How to Configure the Maximum-Prefix Limit

Troubleshooting Tips

If an individual peer or all peers have exceeded the maximum-prefix limit the same number of times as the default or user-defined restart-count value, the individual session or all sessions will need to be manually reset with the `clear ip route`* or `clear eigrp address-family neighbors` command before normal peering can be reestablished.

Configuring the Maximum Number of Prefixes Learned Through Redistribution:
Autonomous System Configuration

The maximum-prefix limit can be configured for prefixes learned through redistribution with the `redistribute maximum-prefix` (EIGRP) command. When the maximum-prefix limit is exceeded, all routes learned from the RIB will be discarded and redistribution will be suspended for the default or user-defined time period. The maximum-prefix limit that can be configured for redistributed prefixes is limited only by the available system resources on the router.

Inherited Timer Values

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the `maximum-prefix` command, are inherited by the `redistribute maximum-prefix` and `neighbor maximum-prefix` command configurations by default. If a single peer is configured with the `neighbor maximum-prefix` command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.
Prerequisites

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

Restrictions

This task can be configured only in IPv4 VRF address family configuration mode.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router eigrp as-number`
4. `address-family ipv4 [unicast] vrf vrf-name`
5. `redistribute maximum-prefix maximum [threshold] [dampened] [reset-time minutes] [restart minutes] [restart-count number] | warning-only`
6. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 router eigrp as-number</td>
<td>Enters router configuration mode and creates an EIGRP routing process.</td>
</tr>
<tr>
<td>Example:</td>
<td>A maximum of 30 EIGRP routing processes can be configured.</td>
</tr>
<tr>
<td>Router(config)# router eigrp 1</td>
<td></td>
</tr>
<tr>
<td>Step 4 address-family ipv4 [unicast] vrf vrf-name</td>
<td>Enters address family configuration mode and creates a session for the VRF.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-router)# address-family ipv4 vrf VRF1</td>
<td></td>
</tr>
</tbody>
</table>
EIGRP Prefix Limit Support

How to Configure the Maximum-Prefix Limit

Command or Action                  Purpose
---                                ---
Step 5  **redistribute maximum-prefix** maximum [threshold] [[dampened] [reset-time minutes] [restart minutes] [restart-count number] [warning-only]]

Limits the number of prefixes redistributed into an EIGRP process.

Example:
```
Router(config-router-af)# redistribute maximum-prefix 10000 80 reset-time 10 restart 2
```

Step 6  **end**

Exits address family configuration mode and enters privileged EXEC mode.

Example:
```
Router(config-router-af)# end
```

Troubleshooting Tips

If the maximum-prefix limit has been exceeded for redistribution the same number of times as the default or user-defined restart-count value, the **clear ip route * or clear ip eigrp neighbors** command will need to be entered before normal redistribution will occur.

Configuring the Maximum Number of Prefixes Learned Through Redistribution: Named Configuration

The maximum-prefix limit can be configured for prefixes learned through redistribution with the **redistribute maximum-prefix** (EIGRP) command. When the maximum-prefix limit is exceeded, all routes learned from the RIB will be discarded and redistribution will be suspended for the default or user-defined time period. The maximum-prefix limit that can be configured for redistributed prefixes is limited only by the available system resources on the router.

Inherited Timer Values

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the **maximum-prefix** command, are inherited by the **redistribute maximum-prefix** and **neighbor maximum-prefix** command configurations by default. If a single peer is configured with the **neighbor maximum-prefix** command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

Prerequisites

VRFs have been created and configured. EIGRP peering is established through the MPLS VPN.

Restrictions

This task can be configured only in IPv4 VRF address family topology configuration mode.
EIGRP Prefix Limit Support

SUMMARY STEPS

1. enable
2. configure terminal
3. router eigrp virtual-instance-name
4. address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number
5. network ip-address [wildcard-mask]
6. topology { base | topology-name tid number }
7. redistribute maximum-prefix maximum [threshold] [[dampened] [reset-time minutes] [restart minutes] [restart-count number] | warning-only]
8. exit-af-topology

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 router eigrp virtual-instance-name</td>
<td>Enters router configuration mode and creates an EIGRP routing process.</td>
</tr>
<tr>
<td>Example: Router(config)# router eigrp virtual-name1</td>
<td></td>
</tr>
<tr>
<td>Step 4 address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
<td>Enters address family configuration mode and creates a session for the VRF.</td>
</tr>
<tr>
<td>Example: Router(config-router)# address-family ipv4 vrf VRF1</td>
<td></td>
</tr>
<tr>
<td>Step 5 network ip-address [wildcard-mask]</td>
<td>Specifies the network for an EIGRP address family routing process.</td>
</tr>
<tr>
<td>Example: Router(config-router-af)# network 172.16.0.0</td>
<td></td>
</tr>
<tr>
<td>Step 6 topology { base</td>
<td>topology-name tid number }</td>
</tr>
<tr>
<td>Example: Router(config-router-af)# topology base</td>
<td></td>
</tr>
</tbody>
</table>
### EIGRP Prefix Limit Support

**How to Configure the Maximum-Prefix Limit**

**Troubleshooting Tips**

If the maximum-prefix limit has been exceeded for redistribution the same number of times as the default or user-defined restart-count value, the `clear ip route *` or `clear eigrp address-family neighbors` command will need to be entered before normal redistribution will occur.

**Configuring the Maximum-Prefix Limit for an EIGRP Process: Autonomous System Configuration**

The maximum-prefix limit can be configured for an EIGRP process to limit the number prefixes that are accepted from all sources. This task is configured with the `maximum-prefix` command. When the maximum-prefix limit is exceeded, sessions with the remote peers are brought down and all routes learned from remote peers are removed from the topology and routing tables. Also, all routes learned from the RIB are discarded and redistribution is suspended for the default or user-defined time period.

**Inherited Timer Values**

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the `maximum-prefix` command, are inherited by the `redistribute maximum-prefix` and `neighbor maximum-prefix` command configurations by default. If a single peer is configured with the `neighbor maximum-prefix` command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

**Prerequisites**

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

**Restrictions**

This task can be configured only in IPv4 VRF address family configuration mode.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>redistribute maximum-prefix maximum [threshold] [[dampened][reset-time minutes][restart minutes][restart-count number][warning-only]]</td>
<td>Limits the number of prefixes redistributed into an EIGRP process.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router-af-topology)# redistribute maximum-prefix 10000 80 reset-time 10 restart 2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>exit-af-topology</td>
<td>Exits address family topology configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-router-af-topology)# exit-af-topology</td>
<td></td>
</tr>
</tbody>
</table>
SUMMARY STEPS

1. enable
2. configure terminal
3. router eigrp as-number
4. address-family ipv4 [unicast] vrf vrf-name
5. maximum-prefix maximum [threshold] [dampened] [reset-time minutes] [restart minutes] [restart-count number] | warning-only
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** router eigrp as-number | Enters router configuration mode and creates an EIGRP routing process.  
  • A maximum of 30 EIGRP routing processes can be configured. |
| **Example:** Router(config)# router eigrp 1 | |
| **Step 4** address-family ipv4 [unicast] vrf vrf-name | Enters address family configuration mode and creates a session for the VRF. |
| **Example:** Router(config-router)# address-family ipv4 vrf RED | |
| **Step 5** maximum-prefix maximum [threshold] [dampened] [reset-time minutes] [restart minutes] [restart-count number] | Limits the number of prefixes that are accepted under an address family by an EIGRP process.  
  • The example configures a maximum-prefix limit of 10,000 prefixes, a reset time period of 10 minutes, a warning message to be displayed at 80 percent of the maximum-prefix limit, and a restart time period of 2 minutes. |
| **Example:** Router(config-router-af)# maximum-prefix 1000080 reset-time 10 restart 2 warning-only | |
| **Step 6** end | Exits address-family configuration mode and enters privileged EXEC mode. |
| **Example:** Router(config-router-af)# end | |
Troubleshooting Tips

If the maximum-prefix limit has been exceeded for redistribution the same number of times as the default or user-defined restart-count value, the `clear ip route *` or `clear ip eigrp neighbors` command will need to be entered before normal redistribution will occur.

Configuring the Maximum-Prefix Limit for an EIGRP Process: Named Configuration

The maximum-prefix limit can be configured for an EIGRP process to limit the number prefixes that are accepted from all sources. This task is configured with the `maximum-prefix` command. When the maximum-prefix limit is exceeded, sessions with the remote peers are brought down and all routes learned from remote peers are removed from the topology and routing tables. Also, all routes learned from the RIB are discarded and redistribution is suspended for the default or user-defined time period.

Inherited Timer Values

Default or user-defined restart, restart-count, and reset-time values for the process-level configuration of this feature, configured with the `maximum-prefix` command, are inherited by the `redistribute maximum-prefix` and `neighbor maximum-prefix` command configurations by default. If a single peer is configured with the `neighbor maximum-prefix` command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

Prerequisites

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

Restrictions

This task can be configured only in IPv4 VRF address family topology configuration mode.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router eigrp virtual-instance-name`
4. `address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
5. `topology { base | topology-name tid number}`
6. `maximum-prefix maximum [threshold] [dampened] [reset-time minutes] [restart minutes] [restart-count number] | warning-only`
7. `exit-af-topology`
8. `show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] accounting`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router eigrp virtual-instance-name</td>
<td>Creates an EIGRP routing process and enters router configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# router eigrp virtual-name1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number</td>
<td>Enters address family configuration mode and creates a session for the VRF.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> topology {base</td>
<td>topology-name tid number}</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af)# topology base</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> maximum-prefix maximum [threshold][[dampened] [reset-time minutes][restart minutes] [restart-count number]</td>
<td>Limits the number of prefixes that are accepted under an address family by an EIGRP process.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af-topology)# maximum-prefix 10000 80 reset-time 10 restart 2 warning-only</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit-af-topology</td>
<td>Exits address family topology configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-router-af-topology)# exit-af-topology</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> show eigrp address-family {ipv4</td>
<td>ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] accounting</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show eigrp address-family ipv4 22 accounting</td>
<td></td>
</tr>
</tbody>
</table>

**Note** Connected and summary routes are not listed individually in the output from this `show` command but are counted in the total aggregate count per process.
Troubleshooting Tips

If the maximum-prefix limit has been exceeded for redistribution the same number of times as the default or user-defined restart-count value, the `clear ip route *` or `clear eigrp address-family neighbors` command will need to be entered before normal redistribution will occur.

Examples

The following is sample output from the `show eigrp address-family accounting` command:

```
Router# show eigrp address-family ipv4 22 accounting

EIGRP-IPv4 VR(saf) Accounting for AS(22)/ID(10.0.0.1)

Total Prefix Count: 3 States: A-Adjacency, P-Pending, D-Down

State Address/Source Interface Prefix Restart Restart/
    Name       Count    Count    Count(s)
A  10.0.0.2  Et0/0      2        0       0
P  10.0.2.4  Se2/0      0        2       114
D  10.0.1.3  Et0/0      0        3       0
```

Configuration Examples for Configuring the Maximum-Prefix Limit

The following examples show how to configure this feature:

- Configuring the Maximum-Prefix Limit for a Single Peer: Autonomous System Configuration Example, page 18
- Configuring the Maximum-Prefix Limit for a Single Peer: Named Example, page 18
- Configuring the Maximum-Prefix Limit for All Peers: Autonomous System Configuration Example, page 18
- Configuring the Maximum-Prefix Limit for All Peers: Named Configuration Example, page 18
- Configuring the Maximum-Prefix Limit for Redistributed Routes: Autonomous System Configuration Example, page 19
- Configuring the Maximum-Prefix Limit for Redistributed Routes: Named Configuration Example, page 19
- Configuring the Maximum-Prefix Limit for an EIGRP Process: Autonomous System Configuration Example, page 20
- Configuring the Maximum-Prefix Limit for an EIGRP Process: Named Configuration Example, page 20
Configuring the Maximum-Prefix Limit for a Single Peer: Autonomous System Configuration Example

The following example, starting in global configuration mode, configures the maximum-prefix limit for a single peer. The maximum limit is set to 1000 prefixes, and the warning threshold is set to 80 percent. When the maximum-prefix limit is exceeded, the session with this peer will be torn down, all routes learned from this peer will be removed from the topology and routing tables, and this peer will be placed in a penalty state for 5 minutes (default penalty value).

Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf VRF1
Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 1000 80
Router(config-router-af)# end

Configuring the Maximum-Prefix Limit for a Single Peer: Named Example

The following example, starting in global configuration mode, configures the maximum-prefix limit for a single peer. The maximum limit is set to 1000 prefixes, and the warning threshold is set to 80 percent. When the maximum-prefix limit is exceeded, the session with this peer will be torn down, all routes learned from this peer will be removed from the topology and routing tables, and this peer will be placed in a penalty state for 5 minutes (default penalty value).

Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 1000 80
Router(config-router-af)# exit-address-family

Configuring the Maximum-Prefix Limit for All Peers: Autonomous System Configuration Example

The following example, starting in global configuration mode, configures the maximum-prefix limit for all peers. The maximum limit is set to 10,000 prefixes, the warning threshold is set to 90 percent, the restart timer is set to 4 minutes, a decay penalty is configured for the restart timer with the dampened keyword, and all timers are configured to be reset to 0 every 60 minutes. When the maximum-prefix limit is exceeded, all peering sessions will be torn down, all routes learned from all peers will be removed from the topology and routing tables, and all peers will be placed in a penalty state for 4 minutes (user-defined penalty value). A dampening exponential decay penalty will also be applied.

Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf VRF1
Router(config-router-af)# neighbor maximum-prefix 10000 90 dampened reset-time 60 restart 4
Router(config-router-af)# end

Configuring the Maximum-Prefix Limit for All Peers: Named Configuration Example

The following example, starting in global configuration mode, configures the maximum-prefix limit for all peers. The maximum limit is set to 10,000 prefixes, the warning threshold is set to 90 percent, the restart timer is set to 4 minutes, a decay penalty is configured for the restart timer with the dampened keyword, and all timers are configured to be reset to 0 every 60 minutes. When the maximum-prefix limit is exceeded, all peering sessions will be torn down, all routes learned from all peers will be removed from the topology and routing tables, and all peers will be placed in a penalty state for 4 minutes (user-defined penalty value). A dampening exponential decay penalty will also be applied.

Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# neighbor maximum-prefix 10000 90 dampened reset-time 60 restart 4
Router(config-router-af)# exit-address-family
keyword, and all timers are configured to be reset to 0 every 60 minutes. When the maximum-prefix limit is exceeded, all peering sessions will be torn down, all routes learned from all peers will be removed from the topology and routing tables, and all peers will be placed in a penalty state for 4 minutes (user-defined penalty value). A dampening exponential decay penalty will also be applied.

Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# neighbor maximum-prefix 10000 90 dampened reset-time 60 restart 4
Router(config-router-af)# exit-address-family

Configuring the Maximum-Prefix Limit for Redistributed Routes: Autonomous System Configuration Example

The following example, starting in global configuration mode, configures the maximum-prefix limit for routes learned through redistribution. The maximum limit is set to 5000 prefixes and the warning threshold is set to 95 percent. When the number of prefixes learned through redistribution reaches 4750 (95 percent of 5000), warning messages will be displayed in the console. Because the warning-only keyword is configured, the topology and routing tables will not be cleared and route redistribution will not be placed in a penalty state.

Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf VRF1
Router(config-router-af)# redistribute maximum-prefix 5000 95 warning-only
Router(config-router-af)# end

Configuring the Maximum-Prefix Limit for Redistributed Routes: Named Configuration Example

The following example, starting in global configuration mode, configures the maximum-prefix limit for routes learned through redistribution. The maximum limit is set to 5000 prefixes and the warning threshold is set to 95 percent. When the number of prefixes learned through redistribution reaches 4750 (95 percent of 5000), warning messages will be displayed in the console. Because the warning-only keyword is configured, the topology and routing tables will not be cleared and route redistribution will not be placed in a penalty state.

Router(config)# router eigrp virtual-name1
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute maximum-prefix 5000 95 warning-only
Router(config-router-af-topology)# exit-af-topology
Configuring the Maximum-Prefix Limit for an EIGRP Process: Autonomous System Configuration Example

The following example, starting in global configuration mode, configures the maximum-prefix limit for an EIGRP process, which includes routes learned through redistribution and routes learned through EIGRP peering sessions. The maximum limit is set to 50,000 prefixes. When the number of prefixes learned through redistribution reaches 37,500 (75 percent of 50,000), warning messages will be displayed in the console.

When the maximum-prefix limit is exceeded, all peering sessions will be reset, the topology and routing tables will be cleared, and redistributed routes and all peering sessions will be placed in a penalty state.

Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# maximum-prefix 50000
Router(config-router-af)# end

Configuring the Maximum-Prefix Limit for an EIGRP Process: Named Configuration Example

The following example, starting in global configuration mode, configures the maximum-prefix limit for an EIGRP process, which includes routes learned through redistribution and routes learned through EIGRP peering sessions. The maximum limit is set to 50,000 prefixes. When the number of prefixes learned through redistribution reaches 37,500 (75 percent of 50,000), warning messages will be displayed in the console.

When the maximum-prefix limit is exceeded, all peering sessions will be reset, the topology and routing tables will be cleared, and redistributed routes and all peering sessions will be placed in a penalty state.

Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# topology base
Router(config-router-af-topology)# maximum-prefix 50000
Router(config-router-af-topology)# exit-af-topology

Additional References

The following sections provide references related to the EIGRP Prefix Limit Support feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP commands</td>
<td>Cisco IOS IP Routing: EIGRP Command Reference</td>
</tr>
<tr>
<td>EIGRP autonomous system configuration and EIGRP named configuration</td>
<td>“Configuring EIGRP” module</td>
</tr>
<tr>
<td>BGP cost community configuration tasks for EIGRP MPLS VPN PE-CE</td>
<td>“BGP Cost Community Support” module</td>
</tr>
<tr>
<td>Basic EIGRP configuration tasks</td>
<td>“Configuring EIGRP” module</td>
</tr>
</tbody>
</table>
## EIGRP Prefix Limit Support

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Feature Information for EIGRP Prefix Limit Support

Table 1 lists the release history for this feature.

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

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

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP Prefix Limit Support</td>
<td>12.0(29)S</td>
<td>The EIGRP Prefix Limit Support feature introduces the capability to limit the number of prefixes per VRF that are accepted from a specific peer or to limit all prefixes that are accepted by an Enhanced Interior Gateway Routing Protocol (EIGRP) process through peering and redistribution.</td>
</tr>
<tr>
<td></td>
<td>12.3(14)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15.0(1)M</td>
<td></td>
</tr>
</tbody>
</table>

The following commands were introduced or modified by this feature: `maximum-prefix`, `neighbor maximum-prefix (EIGRP)`, `redistribute maximum-prefix (EIGRP)`, `show ip eigrp accounting`, `show ip eigrp vrf accounting`.

In Cisco IOS Release 15.0(1)M, the following commands were introduced or modified: `maximum-prefix`, `neighbor description`, `redistribute maximum-prefix (EIGRP)`, `show eigrp address-family accounting`, `show ip eigrp accounting`.

In Cisco IOS Release 15.0(1)M, the following command was replaced: `show ip eigrp vrf accounting`.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2004–2009 Cisco Systems, Inc. All rights reserved.
EIGRP Support for Route Map Filtering

First Published: May 17, 2004
Last Updated: October 2, 2009

The EIGRP Support for Route Map Filtering feature enables Enhanced Interior Gateway Routing Protocol (EIGRP) to interoperate with other protocols to leverage additional routing functionality by filtering inbound and outbound traffic based on complex route map options. Several extended filtering options are introduced to provide EIGRP-specific match choices.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for EIGRP Support for Route Map Filtering” section on page 11.

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

Contents

- Information About EIGRP Support for Route Map Filtering, page 2
- How to Configure EIGRP Support for Route Map Filtering, page 2
- Configuration Examples for EIGRP Support for Route Map Filtering, page 8
- Additional References, page 9
- Feature Information for EIGRP Support for Route Map Filtering, page 11
Information About EIGRP Support for Route Map Filtering

To implement EIGRP route map filtering, you should understand the following concept:

- **EIGRP Route Map Support, page 2**

EIGRP Route Map Support

EIGRP support for route map filtering enables EIGRP to interoperate with other protocols by filtering inbound and outbound traffic based on route map options. Additional EIGRP-specific match choices are available to allow flexibility in fine-tuning EIGRP network operations.

EIGRP supports the route map filtering capability that exists for other routing protocols to filter routes being redistributed into their protocol. For more details about understanding and configuring route maps, see the “Enabling Policy Routing” section of the “Configuring IP Routing Protocol-Independent Features” module of the Cisco IOS IP Routing: Protocol-Independent Configuration Guide.

Match options allow EIGRP to filter internal and external routes based on source protocols, to match a metric against a range, and to match on an external protocol metric.

EIGRP can be configured to filter traffic using a route map and the `redistribute` or `distribute-list` command. Using a route map with the `redistribute` command allows routes that are redistributed from the routing table to be filtered with a route map before being admitted into an EIGRP topology table. Routes that are dynamically received from, or advertised to, EIGRP peers can be filtered by adding a route map option to the `distribute-list` command.

A route map may be configured with both the `redistribute` and the `distribute-list` commands in the same routing process. When a route map is used with a `distribute-list` command that is configured for inbound or outbound filtering, route packets that are learned from or advertised to EIGRP peers can be processed with the route map to provide better control of route selection during the route exchange process. Redistribution serves as a mechanism to import routes into the EIGRP topology table from a routing table. A route map configured with the `redistribute` command adds flexibility to the redistribution capability and results in a more specific redistributed route selection.

The use of route maps to filter traffic is the same for both autonomous-system configurations and named configurations. See the “Configuring EIGRP” module for more information about autonomous system and named configurations.

Demands for EIGRP to interoperate with other protocols and flexibility in fine-tuning network operation necessitate the capability to filter traffic using a route map.

How to Configure EIGRP Support for Route Map Filtering

This section contains the following tasks:

- **Setting EIGRP Tags Using a Route Map for Autonomous System Configurations, page 3** (required)
- **Setting EIGRP Tags Using a Route Map for Named Configurations, page 5**
Setting EIGRP Tags Using a Route Map for Autonomous System Configurations

Perform this task to set EIGRP tags for autonomous system configurations using a route map. The EIGRP metrics used for filtering are configured within a route map. The first match clause defines EIGRP routes that contain an external protocol metric between 400 and 600 inclusive; the second match clause defines EIGRP external routes that match a source protocol of BGP and the autonomous system 45000. When the two match clauses are true, a tag value of the destination routing protocol is set to 5. This route map can be used with the `distribute-list` command; see the “Setting EIGRP Tags Using a Route Map: Autonomous System Configuration Examples” section on page 8 for an example configuration.

SUMMARY STEPS

1. enable
2. configure terminal
3. route-map map-tag [permit | deny] [sequence-number]
4. match metric {metric-value | external metric-value} {+ | - deviation-number}
5. match source-protocol source-protocol [autonomous-system-number]
6. set tag tag-value
7. exit
8. router eigrp as-number
9. network ip-address
10. distribute-list route-map map-tag in

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>route-map map-tag [permit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# route-map metric-range</td>
</tr>
</tbody>
</table>
### Step 4
**match metric** *(metric-value | external metric-value) [+- deviation-number]*

**Example:**
```
Router(config-route-map)# match metric external 500 +- 100
```

**Purpose:** Specifies a match clause that filters inbound updates that match an internal or external protocol metric.
- **metric-value**—Internal protocol metric, which can be an EIGRP five-part metric. The range is from 1 to 4294967295.
- **external**—External protocol metric. The range is from 1 to 4294967295.
- **+- deviation-number**—(Optional) Represents a standard deviation. The deviation can be any number. There is no default.

**Note:** When you specify a metric deviation with the + and - keywords, the router will match any metric that falls inclusively in that range.

**Note:** The external protocol metric is not the same as the EIGRP assigned route metric which is a figure computed from EIGRP vectorized metric components (delay, bandwidth, reliability, load, and MTU).

### Step 5
**match source-protocol** *(source-protocol) [autonomous-system-number]*

**Example:**
```
Router(config-route-map)# match source-protocol bgp 45000
```

**Purpose:** Specifies a match clause that matches external routes from sources that match the source protocol.
- **source-protocol**—Protocol to match. The valid keywords are bgp, connected, eigrp, isis, ospf, rip, and static. There is no default.
- **autonomous-system-number**—(Optional) Autonomous system number. The autonomous-system-number argument is not applicable to the connected, static, and rip keywords. The range is from 1 to 65535. There is no default.

### Step 6
**set tag** *tag-value*

**Example:**
```
Router(config-route-map)# set tag 5
```

**Purpose:** Sets a tag value on the route in the destination routing protocol when all the match criteria of a route map are met.

### Step 7
**exit**

**Example:**
```
Router(config-route-map)# exit
```

**Purpose:** Exits route-map configuration mode and returns to global configuration mode.

### Step 8
**router eigrp** *as-number*

**Example:**
```
Router(config)# router eigrp 1
```

**Purpose:** Configures the EIGRP routing process and enters router configuration mode.
Setting EIGRP Tags Using a Route Map for Named Configurations

Perform this task to set EIGRP tags for named configurations using a route map. The EIGRP metrics used for filtering are configured within a route map. The first match clause defines EIGRP routes that contain an external protocol metric between 400 and 600 inclusive; the second match clause defines EIGRP external routes that match a source protocol of BGP and the autonomous system 45000. When the two match clauses are true, a tag value of the destination routing protocol is set to 5. This route map can be used with the `distribute-list` command, see the “Setting EIGRP Tags Using a Route Map: Named Configuration Examples” section on page 9 for an example configuration.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `route-map map-tag [permit | deny] [sequence-number]`
4. `set metric bandwidth delay reliability loading mtu`
5. `match ip route-source {access-list-number | access-list-name} [...access-list-number | ...access-list-name]`
6. `match metric {metric-value | external metric-value} [+ deviation-number]`
7. `match source-protocol source-protocol [autonomous-system-number]`
8. `set tag source-protocol [autonomous-system-number]`
9. `exit`
10. `router eigrp virtual-instance-name`
11. `address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`  
   or  
   `address-family ipv6 [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`
12. `network ip-address [wildcard-mask]`
13. `af-interface {default | interface-type interface-number}`
14. `next-hop-self eigrp`
15. `topology {base | topology-name tid number}`
16. `distribute-list route-map map-tag in`

**Example:**

Router(config-router)# network 172.16.0.0

Specifies a network for the EIGRP routing process.

**Example:**

Router(config-router)# distribute-list route-map metric-range in

Filters networks received in updates.
## EIGRP Support for Route Map Filtering

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:**  
  Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**  
  Router# configure terminal | |
| **Step 3** route-map map-tag [permit | deny]  
  [sequence-number] | Enters route-map configuration mode. |
| **Example:**  
  Router(config)# route-map metric-range | |
| **Step 4** set metric bandwidth delay reliability loading  
  mtu | (Optional) Sets the metric value for EIGRP in a route map. |
| **Example:**  
  Router(config-route-map)# set metric 10000 10 255 1 1500 | |
| **Step 5** match ip route-source {access-list-number |  
  access-list-name} [...access-list-number |  
  ...access-list-name] | Redistributes routes that have been advertised by routers  
  and access servers at the address specified by the access  
  lists. |
| **Example:**  
  Router(config-route-map)# match ip route-source  
  5 80 | |
| **Step 6** match metric {metric-value | external  
  metric-value} [+ - deviation-number] | Specifies a match clause that includes EIGRP routes that  
  match an internal or external protocol metric.  
  - **metric-value**—Internal protocol metric, which can be  
    an EIGRP five-part metric. The range is from 1 to 4294967295.  
  - **external**—External protocol metric. The range is from 1  
    to 4294967295.  
  - **+ - deviation-number**—(Optional) Represents a  
    standard deviation. The deviation can be any number.  
    There is no default. |
| **Example:**  
  Router(config-route-map)# match metric external  
  500 ++ 100 | **Note**  
  When you specify a metric deviation with the + and -  
  keywords, the router will match any metric that falls  
  inclusively in that range. |
| **Note** The external protocol metric is not the same as the  
  EIGRP assigned route metric, which is a figure  
  computed from EIGRP vectorized metric components (delay,  
  bandwidth, reliability, load, and MTU). |
### Command or Action

**Step 7**

`match source-protocol source-protocol [autonomous-system-number]`

**Purpose**

Specifies a match clause that includes EIGRP external routes that match a source protocol.

- `source-protocol`—Protocol to match. The valid keywords are `bgp`, `connected`, `eigrp`, `isis`, `ospf`, `rip`, and `static`. There is no default.
- `autonomous-system-number`—(Optional) Autonomous system number. The `autonomous-system-number` argument is not applicable to the `connected`, `static`, and `rip` keywords. The range is from 1 to 65535. There is no default.

**Example:**

```
Router(config-route-map)# match source-protocol bgp 45000
```

**Step 8**

`set tag tag-value`

**Purpose**

Sets a tag value on the route in the destination routing protocol when all the match criteria of a route map are met.

**Example:**

```
Router(config-route-map)# set tag 5
```

**Step 9**

`exit`

**Purpose**

Exits route-map configuration mode and returns to global configuration mode.

**Example:**

```
Router(config-route-map)# exit
```

**Step 10**

`router eigrp virtual-instance-name`

**Purpose**

Configures the EIGRP routing process and enters router configuration mode.

**Example:**

```
Router(config)# router eigrp virtual-name1
```

**Step 11**

`address-family ipv4 [multicast] [unicast] [vrf vrf-name] autonomous-system autonomous-system-number`

**Purpose**

Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

**Example:**

```
Router(config-router)# address-family ipv4 autonomous-system 45000
```

**Step 12**

`network ip-address [wildcard-mask]`

**Purpose**

Specifies a network for the EIGRP routing process.

**Example:**

```
Router(config-router-af)# network 172.16.0.0
```

**Step 13**

`af-interface {default | interface-type interface-number}`

**Purpose**

Enters address family interface configuration mode to configure interface-specific EIGRP commands.

**Example:**

```
Router(config-router-af)# af-interface default
```
### Configuration Examples for EIGRP Support for Route Map Filtering

This section contains the following configuration examples:

- Setting EIGRP Tags Using a Route Map: Autonomous System Configuration Examples, page 8
- Setting EIGRP Tags Using a Route Map: Named Configuration Examples, page 9

#### Setting EIGRP Tags Using a Route Map: Autonomous System Configuration Examples

The following example shows how to configure a route map to match an EIGRP external protocol metric route with an allowable deviation of 100, a source protocol of BGP, and an autonomous system 45000. When the two match clauses are true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process.

```
Router(config)# route-map metric-range
Router(config-route-map)# match metric external 500 +- 100
Router(config-route-map)# match source-protocol bgp 45000
Router(config-route-map)# set tag 5
Router(config-route-map)# exit
```

The following example shows how to configure a route map to match EIGRP routes with a metric of 110, 200, or an inclusive range of 700 to 800. When the match clause is true, the tag value of the destination routing protocol is set to 10. The route map is used to redistribute EIGRP packets.

```
Router(config)# route-map metric-eigrp
Router(config-route-map)# match metric 110 200 750 +- 50
Router(config-route-map)# set tag 10
Router(config-route-map)# exit
```

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 14 next-hop-self eigrp</td>
<td>Enables EIGRP to advertise routes with the local outbound interface address as the next hop.</td>
</tr>
<tr>
<td>Step 15 topology [base</td>
<td>topology-name tid number]</td>
</tr>
<tr>
<td>Step 16 distribute-list route-map map-tag in</td>
<td>Filters networks received in updates.</td>
</tr>
</tbody>
</table>
Setting EIGRP Tags Using a Route Map: Named Configuration Examples

The following example shows how to configure a route map to match an EIGRP external protocol metric route with an allowable deviation of 100, a source protocol of BGP, and an autonomous system 45000. When the two match clauses are true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process.

```
Router(config)# route-map metric_range
Router(config-route-map)# match metric external 500 +- 100
Router(config-route-map)# match source-protocol bgp 45000
Router(config-route-map)# set tag 5
Router(config-route-map)# exit
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# network 172.21.1.0/24
Router(config-router-af-topology)# topology base
Router(config-router-af-topology)# distribute-list route-map metric_range in
```

The following example shows how to configure a route map to match EIGRP routes with a metric of 110, 200, or an inclusive range of 700 to 800. When the match clause is true, the tag value of the destination routing protocol is set to 10. The route map is used to redistribute EIGRP packets.

```
Router(config)# route-map metric_eigrp
Router(config-route-map)# match metric 110 200 750 +- 50
Router(config-route-map)# set tag 10
Router(config-route-map)# exit
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# network 172.21.1.0/24
Router(config-router-af-topology)# topology base
Router(config-router-af-topology)# distribute-list route-map metric-range in
```

Additional References

The following sections provide references related to the EIGRP Support for Route Map Filtering feature.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP overview and configuration</td>
<td>“Configuring EIGRP” module</td>
</tr>
<tr>
<td>IP routing commands including syntax, usage guidelines, and examples</td>
<td><em>Cisco IOS IP Routing Protocols Command Reference</em></td>
</tr>
</tbody>
</table>

**Standards**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Feature Information for EIGRP Support for Route Map Filtering

Table 1 lists the release history for this feature.

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

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

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

Table 1 Feature Information for EIGRP Support for Route Map Filtering

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP Support for Route Map Filtering</td>
<td>12.2(33)SRA 12.2(33)SXH 12.3(8)T 15.0(1)M</td>
<td>The EIGRP Support for Route Map Filtering feature enables EIGRP to interoperate with other protocols by filtering inbound and outbound traffic based on complex route map options. Several extended filtering options are introduced to provide EIGRP-specific match choices. The following commands were introduced or modified by this feature: <strong>match metric (IP)</strong>, <strong>match source-protocol</strong>, <strong>show ip eigrp topology</strong>. In Cisco IOS Release 15.0(1)M, the following command was introduced or modified for this feature: <strong>show eigrp address-family topology</strong></td>
</tr>
</tbody>
</table>

© 2004–2009 Cisco Systems, Inc. All rights reserved.