CISCO.

CCNA Learning

Authorized Self-Study Guide

Interconnecting Cisco Network Devices, Part 2 (ICND2)

Third Edition

Foundation learning for CCNA ICND2 Exam 640-816

ciscopress.com

Steve McQuerry, CCIE® No. 6108

Authorized Self-Study Guide
Interconnecting Cisco Network Devices, Part 2 (ICND2)

Steve McQuerry

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing February 2008

Library of Congress Cataloging-in-Publication Data:

McQuerry, Steve.

Interconnecting Cisco network devices. Part 2 (ICND2) / Steve McQuerry.

p. cm.

ISBN 978-1-58705-463-1 (hardback)

1. Internetworking (Telecommunication)—Examinations—Study guides. 2. Computer networks—Problems, exercises, etc. 3. Telecommunications engineers—Certification—Examinations—Study guides. I. Title.

TK5105.5.M33992 2008

004.6—dc22

2008000513

ISBN-13: 978-1-58705-463-1

ISBN-10: 1-58705-463-9

Warning and Disclaimer

This book is designed to provide information about the configuration and operation of Cisco routers and switches as described in the Interconnecting Cisco Network Devices 2 (ICND2) course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Foreword

Cisco certification self-study guides are excellent self-study resources for networking professionals to maintain and increase internetworking skills, and to prepare for Cisco Career Certification exams. Cisco Career Certifications are recognized worldwide and provide valuable, measurable rewards to networking professionals and their employers.

Cisco Press exam certification guides and preparation materials offer exceptional—and flexible—access to the knowledge and information required to stay current in one's field of expertise, or to gain new skills. Whether used to increase internetworking skills or as a supplement to a formal certification preparation course, these materials offer networking professionals the information and knowledge required to perform on-the-job tasks proficiently.

Developed in conjunction with the Cisco certifications and training team, Cisco Press books are the only self-study books authorized by Cisco, and they offer students a series of exam practice tools and resource materials to help ensure that learners fully grasp the concepts and information presented.

Additional authorized Cisco instructor-led courses, e-learning, labs, and simulations are available exclusively from Cisco Learning Solutions Partners worldwide. To learn more, visit http://www.cisco.com/go/training.

I hope you will find this guide to be an essential part of your exam preparation and professional development, as well as a valuable addition to your personal library.

Drew Rosen
Manager, Learning & Development
Learning@Cisco
December 2007

Introduction

Since the introduction of the personal computer in the early 1970s, businesses have found more uses and applications for technology in the workplace. With the introduction of local-area networks, file sharing, and print sharing in the 1980s, it became obvious that distributed computing was no longer a passing fad. By the 1990s, computers became less expensive, and innovations such as the Internet allowed everyone to connect to computer services worldwide. Computing services have become large and distributed. The days of punch cards and green-bar paper are behind us, and a new generation of computing experts is being asked to keep this distributed technology operational. These experts are destined to have a new set of issues and problems to deal with, the most complex of them being connectivity and compatibility among differing systems and devices.

The primary challenge with data networking today is to link multiple devices' protocols and sites with maximum effectiveness and ease of use for end users. Of course, this must all be accomplished in a cost-effective way. Cisco offers a variety of products to give network managers and analysts the ability to face and solve the challenges of internetworking.

In an effort to ensure that these networking professionals have the knowledge to perform these arduous tasks, Cisco has developed a series of courses and certifications that act as benchmarks for internetworking professionals. These courses help internetworking professionals learn the fundamentals of internetworking technologies along with skills in configuring and installing Cisco products. The certification exams are designed to be a litmus test for the skills required to perform at various levels of internetworking. The Cisco certifications range from the associate level, Cisco Certified Network Associate (CCNA), through the professional level, Cisco Certified Network Professional (CCNP), to the expert level, Cisco Certified Internetwork Expert (CCIE).

The Interconnecting Cisco Network Devices, Part 2 (ICND2) course is one of two recommended training classes for CCNA preparation. As a self-study complement to the course, this book helps to ground individuals in the fundamentals of switches and routed internetworks.
It presents the concepts, commands, and practices required to configure Cisco switches and routers to operate in corporate internetworks. You will be introduced to all the basic concepts and configuration procedures required to build a multiswitch, multirouter, and multigroup internetwork that uses LAN and WAN interfaces for the most commonly used routing and routed protocols. ICND provides the installation and configuration information that network administrators require to install and configure Cisco products.

Interconnecting Cisco Network Devices, Part 2 (ICND2), is the second part of a two-part, introductory-level series and is recommended for individuals who have one to three years of internetworking experience, are familiar with basic internetworking concepts, and have basic experience with the TCP/IP protocol. While the self-study book is designed for those who are pursuing the CCNA certification, it is also useful for network administrators responsible for implementing and managing small- and medium-sized business networks. Network support staff who perform a help-desk role in a medium- or enterprise-sized company will find this a valuable resource. Finally, Cisco customers or channel resellers and network technicians entering the internetworking industry who are new to Cisco products can benefit from the contents of this book.

Goals

The goal of this book is twofold. First, it is intended as a self-study book for the ICND2 test 640-816 and the CCNA test 640-802, which are part of the requirements for the CCNA certification. Like the certification itself, the book should help readers become literate in the use of switches, routers, and the associated protocols and technologies. The second goal is that someone who completes the book and the CCNA certification should be able to use these skills to select, connect, and configure Cisco devices in an internetworking environment. In particular, the book covers the basic steps and processes involved with moving data through the network using routing and Layer 2 switching.

Readers interested in more information about the CCNA certification should consult the Cisco website at http://www.cisco.com/en/US/learning/le3/le2/le0/le9/learning_certification_type_home.html. To schedule a Cisco certification test, contact Pearson Vue on the web at http://www.PearsonVue.com/cisco or Prometric on the web at http://www.2test.com.

Chapter Organization

This book is divided into eight chapters and an appendix and is designed to be read in order because many chapters build on content from previous chapters.

- Chapter 1, "Review of Cisco IOS for Routers and Switches," provides a review of the Cisco IOS. This is an assumed knowledge for readers, but this chapter provides a brief review of command structure that is used throughout the other chapters of the book.

- Chapter 2, “Medium-Sized Switched Network Construction,” explores the operation and configuration of local-area networks, including the challenges associated with these networks, and describes how network devices are used to eliminate these problems focusing on Layer 2 switching.
- Chapter 3, “Medium-Sized Routed Network Construction,” describes routing operations. This chapter discusses the differences between link-state and distance vector routing protocols and provides the foundation for Chapters 4 and 5.
- Chapter 4, “Single-Area OSPF Implementation,” looks at how to configure OSPF to act as a routing protocol within a network. This chapter describes the operation of the protocol and provides configuration examples for a single area. The chapter also includes troubleshooting steps.
- Chapter 5, “Implementing EIGRP,” discusses the EIGRP routing protocol. It describes the operation of the protocol and the configuration requirements. It also includes troubleshooting steps.
- Chapter 6, “Managing Traffic with Access Control Lists,” discusses how access control lists are used in Cisco IOS to identify and filter traffic. The chapter discusses the configuration of the lists and provides some practical applications of these lists.
- Chapter 7, “Managing Address Spaces with NAT and IPv6,” discusses the limitations of IPv4 address space, specifically that these addresses are running out. The chapter discusses how Network Address Translation (NAT) and Port Address Translation (PAT) are helping conserve addresses and how IPv6 will alleviate this problem. The chapter also discusses the configuration of NAT, PAT, and IPv6.
- Chapter 8, “Extending the Network into the WAN,” describes how different sites can be connected across a wide-area network or using the Internet. It discusses VPN and SSL VPN (WebVPN) solutions as well as traditional leased line and Frame Relay connections. The chapter also provides a troubleshooting section.
- The appendix, “Answers to Chapter Review Questions,” provides answers to the review questions at the end of each chapter.

Features

This book features actual router and switch output to aid in the discussion of the configuration of these devices. Many notes, tips, and cautions are also spread throughout the text. In addition, you can find many references to standards, documents, books, and websites to help you understand networking concepts. At the end of each chapter, your comprehension and knowledge are tested by review questions prepared by a certified Cisco instructor.

NOTE The operating systems used in this book are Cisco IOS Software Release 12.4 for the routers, and Cisco Catalyst 2960 is based on Cisco IOS Software Release 12.2.

CHAPTER 5

Implementing EIGRP

This chapter discusses the features of Enhanced Interior Gateway Routing Protocol (EIGRP), a Cisco routing protocol that is designed to address the shortcomings of both distance vector and link-state routing protocols. The text expands on the underlying technologies in EIGRP, including the path selection process.

Chapter Objectives

Upon completing this chapter, you will be able to configure, verify, and troubleshoot EIGRP. This ability includes being able to meet these objectives:

- Describe the operation and configuration of EIGRP, including load balancing and authentication
- Identify an approach for troubleshooting common EIGRP problems and offer solutions

Implementing EIGRP

EIGRP is an advanced distance vector routing protocol developed by Cisco. EIGRP is suited for many different topologies and media. In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal overhead. EIGRP is a popular choice for a routing protocol on Cisco devices.

Introducing EIGRP

EIGRP is a Cisco-proprietary routing protocol that combines the advantages of link-state and distance vector routing protocols. EIGRP is an advanced distance vector or hybrid routing protocol that includes the following features:

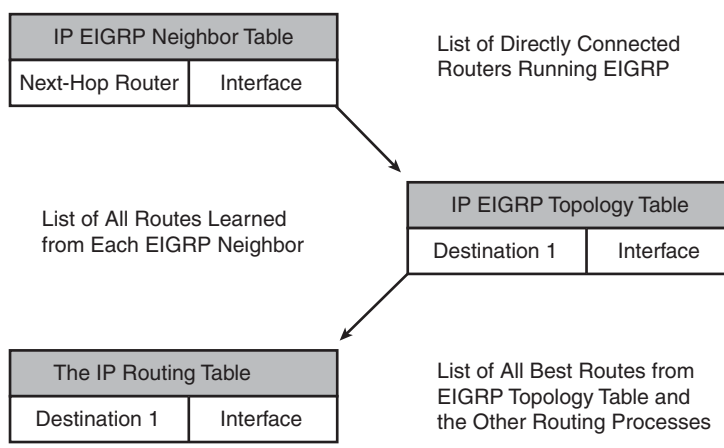
- **Rapid convergence:** EIGRP uses the Diffusing Update Algorithm (DUAL) to achieve rapid convergence. A router that uses EIGRP stores all available backup routes for destinations so that it can quickly adapt to alternate routes. If no appropriate route or backup route exists in the local routing table, EIGRP queries its neighbors to discover an alternate route.

- **Reduced bandwidth usage:** EIGRP does not make periodic updates. Instead, it sends partial updates when the path or the metric changes for that route. When path information changes, DUAL sends an update about only that link rather than about the entire table.
- **Multiple network layer support:** EIGRP supports AppleTalk, IP version 4 (IPv4), IP version 6 (IPv6), and Novell Internetwork Packet Exchange (IPX), which use protocol-dependent modules (PDM). PDMs are responsible for protocol requirements that are specific to the network layer.
- **Classless routing:** Because EIGRP is a classless routing protocol, it advertises a routing mask for each destination network. The routing mask feature enables EIGRP to support discontiguous subnetworks and variable-length subnet masks (VLSM).
- **Less overhead:** EIGRP uses multicast and unicast rather than broadcast. As a result, end stations are unaffected by routing updates and requests for topology information.
- **Load balancing:** EIGRP supports unequal metric load balancing, which allows administrators to better distribute traffic flow in their networks.
- **Easy summarization:** EIGRP enables administrators to create summary routes anywhere within the network rather than rely on the traditional distance vector approach of performing classful route summarization only at major network boundaries.

Each EIGRP router maintains a neighbor table. This table includes a list of directly connected EIGRP routers that have an adjacency with this router.

Each EIGRP router maintains a topology table for each routed protocol configuration. The topology table includes route entries for every destination that the router learns. EIGRP chooses the best routes to a destination from the topology table and places these routes in the routing table, as illustrated in Figure 5-1.

Figure 5-1 *EIGRP Tables*



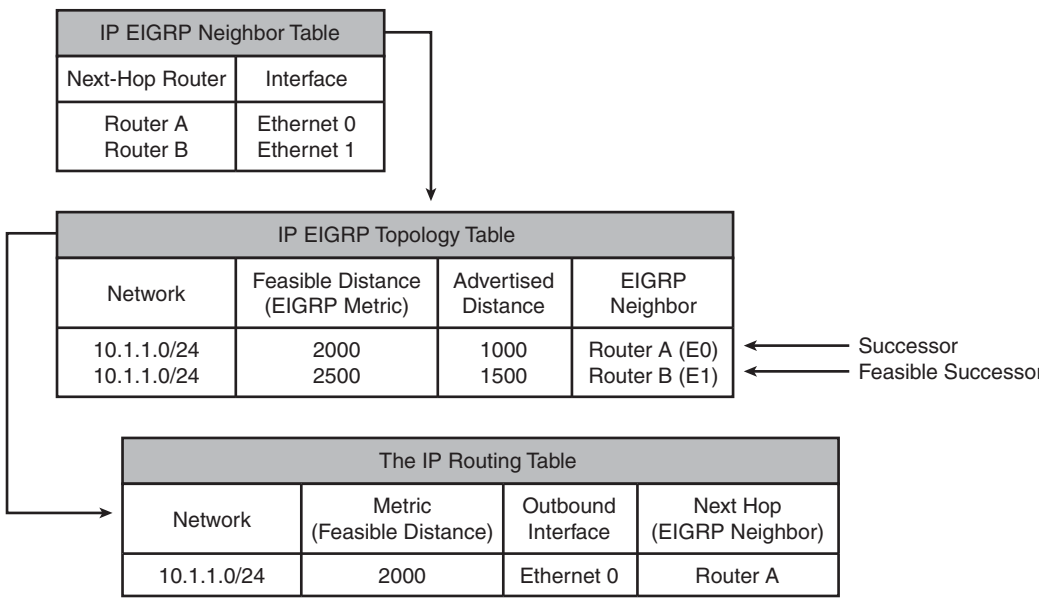
In EIGRP, the best route is called a *successor route* while a backup route is called the *feasible successor*. To determine the best route (successor) and the backup route (feasible successor) to a destination, EIGRP uses the following two parameters:

- **Advertised distance:** The EIGRP metric for an EIGRP neighbor to reach a particular network
- **Feasible distance:** The advertised distance for a particular network learned from an EIGRP neighbor plus the EIGRP metric to reach that neighbor

A router compares all feasible distances to reach a specific network and then selects the lowest feasible distance and places it in the routing table. The feasible distance for the chosen route becomes the EIGRP routing metric to reach that network in the routing table.

The EIGRP topology database contains all the routes that are known to each EIGRP neighbor. Routers A and B send their routing tables to Router C, whose table is displayed in Figure 5-2. Both Routers A and B have pathways to network 10.1.1.0/24, as well as to other networks that are not shown.

Figure 5-2 *Router C EIGRP Tables*



Router C has two entries to reach 10.1.1.0/24 in its topology table. The EIGRP metric for Router C to reach both Routers A and B is 1000. Add this cost (1000) to the respective advertised distance

for each router, and the results represent the feasible distances that Router C must travel to reach network 10.1.1.0/24.

Router C chooses the least-cost feasible distance (2000) and installs it in the IP routing table as the best route to reach 10.1.1.0/24. The route with the least-cost feasible distance that is installed in the routing table is called the *successor route*.

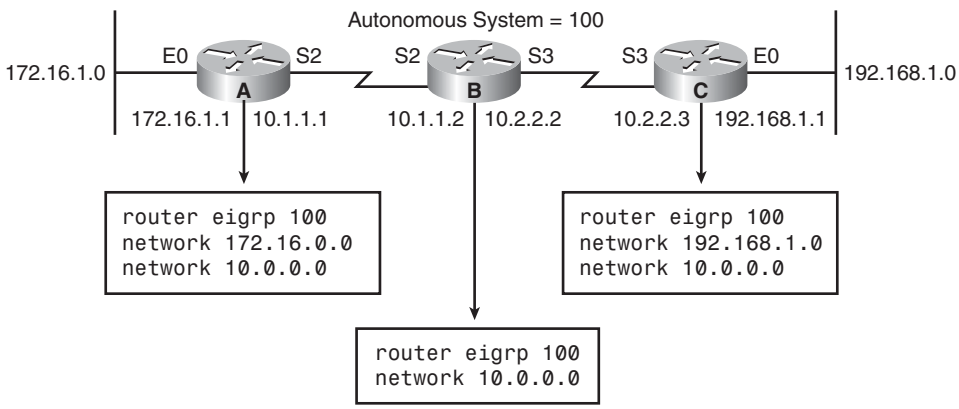
Router C then chooses a backup route to the successor called a *feasible successor route*, if one exists. For a route to become a feasible successor, a next-hop router must have an advertised distance that is less than the feasible distance of the current successor route.

If the route through the successor becomes invalid, possibly because of a topology change, or if a neighbor changes the metric, DUAL checks for feasible successors to the destination route. If one is found, DUAL uses it, avoiding the need to recompute the route. If no feasible successor exists, a recomputation must occur to determine the new successor.

Configuring and Verifying EIGRP

Use the **router eigrp** and **network** commands to create an EIGRP routing process. Note that EIGRP requires an autonomous system (AS) number. The AS number does not have to be registered as is the case when routing on the Internet with the Border Gateway Protocol (BGP) routing protocol. However, all routers within an AS must use the same AS number to exchange routing information with each other. Figure 5-3 shows the EIGRP configuration of a simple network.

Figure 5-3 *EIGRP Configuration*



The **network** command defines a major network number to which the router is directly connected. The EIGRP routing process looks for interfaces that have an IP address that belongs to the

networks that are specified with the **network** command and begins the EIGRP process on these interfaces.

Table 5-1 applies to the EIGRP configurations on Router A in the EIGRP configuration example.

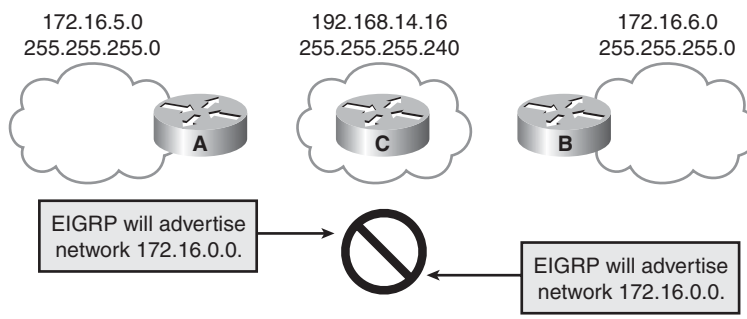
Table 5-1 *EIGRP Command Example*

Command	Description
router eigrp 100	Enables the EIGRP routing process for AS 100
network 172.16.0.0	Associates network 172.16.0.0 with the EIGRP routing process
network 10.0.0.0	Associates network 10.0.0.0 with the EIGRP routing process

EIGRP sends updates out of the interfaces in networks 10.0.0.0 and 172.16.0.0. The updates include information about networks 10.0.0.0 and 172.16.0.0 and any other networks that EIGRP learns.

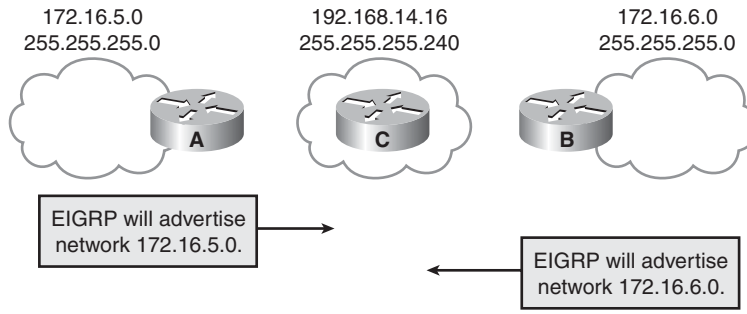
EIGRP automatically summarizes routes at the classful boundary. In some cases, you might not want automatic summarization to occur. For example, if you have discontiguous networks, you need to disable automatic summarization to minimize router confusion. Figure 5-4 shows an example of how this summarization can cause advertisements for the 172.16.0.0 network to be sent from both Router A and Router B to Router C.

Figure 5-4 *Autosummarization Causing Discontinuous Subnets*



To disable automatic summarization, use the **no auto-summary** command in the EIGRP router configuration mode. When this command is used, both Router A and Router B will advertise the route specific to the subnet of a given interface, as shown in Figure 5-5.

Figure 5-5 *Disabling Autosummarization Corrects Problem*



After you enable EIGRP, various commands can be used to display information about how the protocol is operating. The **show ip route eigrp** command displays the current EIGRP entries in the routing table.

The **show ip protocols** command displays the parameters and current state of the active routing protocol process. This command shows the EIGRP AS number. It also displays filtering and redistribution numbers and neighbor and distance information. This also shows the networks that are currently being advertised on the router by the protocol.

Use the **show ip eigrp interfaces** [*type number*] [*as-number*] command to determine on which interfaces EIGRP is active, and to learn information about EIGRP that relates to those interfaces. If you specify an interface by using the *type number* option, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed. If you specify an AS using the *as-number* option, only the routing process for the specified AS is displayed. Otherwise, all EIGRP processes are displayed. Example 5-1 shows the output of the **show ip eigrp interfaces** command.

Example 5-1 *Determining Router Interface EIGRP Status/Information*

```
RouterX# show ip eigrp interfaces
IP EIGRP interfaces for process 109

                    Xmit Queue    Mean   Pacing Time   Multicast    Pending
Interface  Peers    Un/Reliable   SRTT   Un/Reliable   Flow Timer   Routes
Di0        0        0/0           0      11/434        0            0
Et0        1        0/0           337    0/10          0            0
SE0:1.16   1        0/0           10     1/63          103          0
Tu0        1        0/0           330    0/16          0            0
```

Table 5-2 describes the significant fields generated by the **show ip eigrp interfaces** output.

Table 5-2 **show ip eigrp interfaces** *Output*

Field	Description
Interface	Interface over which EIGRP is configured
Peers	Number of directly connected EIGRP neighbors on the interface
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable queues
Mean SRTT	Average smoothed round-trip time (SRTT) interval (in milliseconds) for all neighbors on the interface
Pacing Time Un/Reliable	Number of milliseconds to wait after transmitting unreliable and reliable packets
Multicast Flow Timer	Number of milliseconds to wait for acknowledgment of a multicast packet by all neighbors before transmitting the next multicast packet
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent

Use the **show ip eigrp neighbors** command to display the neighbors that were discovered by EIGRP and to determine when neighbors become active and inactive, as demonstrated in Example 5-2. This command is also useful for debugging certain types of transport problems.

Example 5-2 *Displaying Discovered Active/Inactive EIGRP Neighbors*

```
RouterX# show ip eigrp neighbors
IP-EIGRP Neighbors for process 77
Address         Interface     Holdtime        Uptime    Q      Seq   SRTT     RTO
                              (secs)          (h:m:s)   Count  Num   (ms)     (ms)
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
```

Table 5-3 describes the significant fields for the **show ip eigrp neighbors** command.

Table 5-3 **show ip eigrp neighbors** *Output*

Field	Description
process 77	AS number that is specified with the **router** command.
Address	IP address of the EIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Holdtime	Length of time (in seconds) that Cisco IOS Software waits to hear from the peer before declaring it down. If the peer is using the default hold time, this number is less than 15. If the peer configures a nondefault hold time, the nondefault hold time is displayed. The hold time would be less than 180 on a sub-T1 multipoint interface.
Uptime	Elapsed time (in hours:minutes:seconds) since the local router first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the software is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.
SRTT	Smooth round-trip time (SRTT). The number of milliseconds that is required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout (RTO) (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.

The **show ip eigrp topology** command displays the EIGRP topology table, the active or passive state of routes, the number of successors, and the feasible distance to the destination, as demonstrated in Example 5-3.

Example 5-3 *Displaying EIGRP Topology Information*

```
RouterX# show ip eigrp topology
IP-EIGRP Topology Table for process 77
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 172.16.90.0 255.255.255.0, 2 successors, FD is 46251776
          via 172.16.80.28 (46251776/46226176), Ethernet0
          via 172.16.81.28 (46251776/46226176), Ethernet1
          via 172.16.80.31 (46277376/46251776), Serial0
P 172.16.81.0 255.255.255.0, 2 successors, FD is 307200
          via Connected, Ethernet1
          via 172.16.81.28 (307200/281600), Ethernet1
          via 172.16.80.28 (307200/281600), Ethernet0
          via 172.16.80.31 (332800/307200), Serial0
```

Table 5-4 describes the significant fields for the **show ip eigrp topology** command output.

Table 5-4 **show ip eigrp topology** *Output*

Field	Description
Codes	The state of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P - Passive	Indicates that no EIGRP computations are being performed for this destination.
A - Active	Indicates that EIGRP computations are being performed for this destination.
U - Update	Indicates that an update packet was sent to this destination.
Q - Query	Indicates that a query packet was sent to this destination.
R - Reply	Indicates that a reply packet was sent to this destination.
r - Reply status	A flag that is set after the software has sent a query and is waiting for a reply.
172.16.90.0	Destination IP network number.
255.255.255.0	Destination subnet mask.
successors	Number of successors. This number corresponds to the number of next hops in the IP routing table. If "successors" is capitalized, the route or next hop is in a transition state.
FD	Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. After the software determines it has a feasible successor, it does not need to send a query for that destination.
replies	The number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in active state.
state	The exact EIGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is in the active state.
via	The IP address of the peer that told the software about this destination. The first *n* of these entries, where *n* is the number of successors, are the current successors. The remaining entries on the list are feasible successors.
(46251776/ 46226176)	The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.
Ethernet0	The interface from which this information was learned.
Serial0	The interface from which this information was learned.

The **show ip eigrp traffic** command displays the number of packets sent and received, as demonstrated in Example 5-4.

Example 5-4 *Displaying the Number of EIGRP Sent/Received Packets*

```
RouterX# show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 77
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
```

Table 5-5 describes the fields that might be shown in the display.

Table 5-5 **show ip eigrp traffic** *Output*

Field	Description
process 77	The AS number that is specified in the **router** command
Hellos sent/received	The number of hello packets that were sent and received
Updates sent/received	The number of update packets that were sent and received
Queries sent/received	The number of query packets that were sent and received
Replies sent/received	The number of reply packets that were sent and received
Acks sent/received	The number of acknowledgment packets that were sent and received

The **debug ip eigrp** privileged EXEC command helps you analyze the EIGRP packets that an interface sends and receives, as demonstrated in Example 5-5. Because the **debug ip eigrp** command generates a substantial amount of output, use it only when traffic on the network is light.

Example 5-5 *Analyzing Sent/Received EIGRP Packets*

```
RouterX# debug ip eigrp
IP-EIGRP: Processing incoming UPDATE packet
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP: Ext 192.168.0.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 -
256000 104960
IP-EIGRP: 172.69.43.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.43.0 255.255.255.0 metric 371200 - 256000 115200
IP-EIGRP: 192.135.246.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.246.0 255.255.255.0 metric 46310656 - 45714176 596480
IP-EIGRP: 172.69.40.0 255.255.255.0, - do advertise out Ethernet0/1
```

Example 5-5 *Analyzing Sent/Received EIGRP Packets (Continued)*

```
IP-EIGRP: Ext 172.69.40.0 255.255.255.0 metric 2272256 - 1657856 614400
IP-EIGRP: 192.135.245.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.245.0 255.255.255.0 metric 40622080 - 40000000 622080
IP-EIGRP: 192.135.244.0 255.255.255.0, - do advertise out Ethernet0/1
```

Table 5-6 describes the fields in the sample output from the **debug ip eigrp** command.

Table 5-6 **debug ip eigrp** *Output*

Field	Description
IP-EIGRP	Indicates that this is an IP EIGRP packet.
Ext	Indicates that the following address is an external destination rather than an internal destination, which would be labeled as Int.
do not advertise out	Indicates interfaces out which EIGRP will not advertise the given route. This configuration prevents routing loops (split horizon).
M	Displays the computed metric, which includes the sent metric (SM) and the cost between this router and the neighbor. The first number is the composite metric. The next two numbers are the inverse bandwidth and the delay, respectively.
SM	Displays the metric as reported by the neighbor.

Load Balancing with EIGRP

Typically, networks are configured with multiple paths to a remote network. When these paths are equal or nearly equal, it makes sense to utilize all the available paths. Unlike Layer 2 forwarding, Layer 3 forwarding has the capability to load-balance between multiple paths. That is, the router can send frames out multiple interfaces to reduce the amount of traffic sent to a single network connection. The key to this feature is that the network paths must be of equal cost (or nearly equal for some protocols like EIGRP). EIGRP uses a metric to compute the costs to a given network.

EIGRP Metric

The EIGRP metric can be based on several criteria, but EIGRP uses only two of these criteria by default:

- **Bandwidth:** The smallest bandwidth between source and destination
- **Delay:** The cumulative interface delay in microseconds along the path

The following criteria can be used but are not recommended because they typically result in frequent recalculation of the topology table:

- **Reliability:** This value represents the worst reliability between the source and destination, based on keepalives.
- **Load:** This value represents the worst load on a link between the source and destination, computed based on the packet rate and the configured bandwidth of the interface.

NOTE Although the maximum transmission unit (MTU) is exchanged in EIGRP packets between neighbor routers, MTU is not factored into the EIGRP metric calculation.=

Load Balancing Across Equal Paths

Equal-cost load balancing is the capability of a router to distribute traffic over all its network ports that are the same metric from the destination address. Load balancing increases the use of network segments and increases effective network bandwidth.

For IP, Cisco IOS Software applies load balancing across up to four equal-cost paths by default. With the **maximum-paths** *maximum-path* router configuration command, up to 16 equal-cost routes can be kept in the routing table. If you set the *maximum-path* to 1, you disable load balancing. When a packet is process switched, load balancing over equal-cost paths occurs on a per-packet basis. When packets are fast switched, load balancing over equal-cost paths occurs on a per-destination basis.

NOTE If you test load balancing, do not ping to or from routers that use fast-switching interfaces because these router-generated packets are process switched rather than fast switched and might produce confusing results.

Configuring Load Balancing Across Unequal-Cost Paths

EIGRP can also balance traffic across multiple routes that have different metrics, which is called unequal-cost load balancing. The degree to which EIGRP performs load balancing is controlled with the **variance** command.

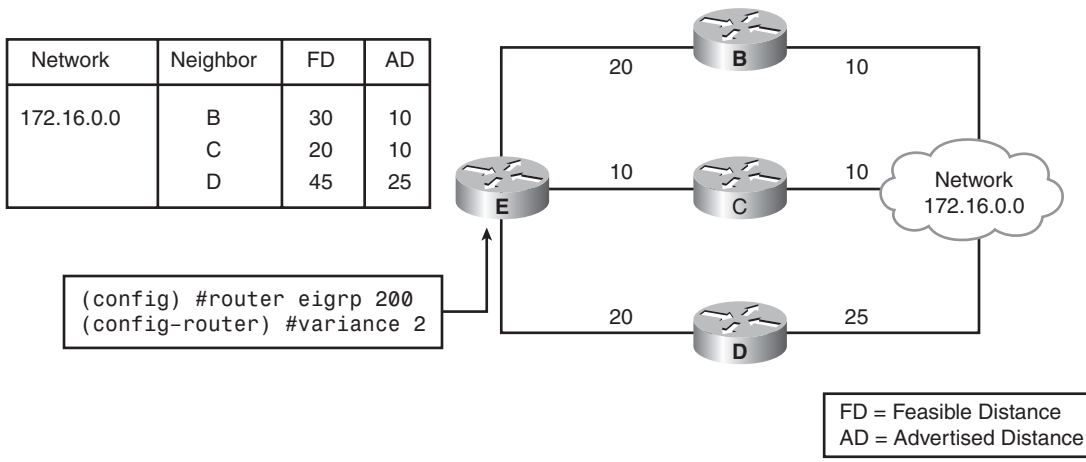
The *multiplier* parameter for the **variance** command is a value from 1 to 128, used for load balancing. The default is 1, which indicates that only equal-cost load balancing is being performed. The multiplier defines the range of metric values that are accepted for load balancing by the EIGRP process.

NOTE By default, traffic is distributed proportionately among the links with unequal costs, with respect to the metric.

Example: Variance

In Figure 5-6, a variance of 2 is configured, and the range of the metric values, which are the feasible distances for Router E to get to network 172.16.0.0, is 20 to 45. This range of values determines the feasibility of a potential route.

Figure 5-6 *Variance Example*



A route is feasible if the next router in the path is closer to the destination than to the current router and if the metric of the alternate path is within the variance. Load balancing can use only feasible paths, and the routing table includes only these paths. The two feasibility conditions are as follows:

- The local best metric, which is the current feasible distance, must be greater than the best metric (the advertised distance) that is learned from the next router. In other words, the next router in the path must be closer to the destination than to the current router; this criterion prevents routing loops.
- The metric of the alternate path must be less than the variance multiplied by the local best metric (the current feasible distance).

If both of these conditions are met, the route is determined to be feasible and can be added to the routing table.

In Figure 5-6, three paths to network 172.16.0.0 exist with the following metrics:

- **Path 1:** 30 (through B)
- **Path 2:** 20 (through C)
- **Path 3:** 45 (through D)

By default, the router places only path 2 (through C) in the routing table because it is the least-cost path. To load-balance over paths 1 and 2, use a variance of 2 because 20 * 2 = 40, which is greater than the metric through path 1.

In Figure 5-6, Router E uses Router C as the successor because it has the lowest feasible distance (20). With the **variance 2** command applied to Router E, the path through Router B meets the criteria for load balancing. In this case, the feasible distance through Router B is less than twice the feasible distance for the successor (Router C).

Router D is not considered for load balancing with this variance because the feasible distance through Router D is greater than twice the feasible distance for the successor (Router C). In the example, however, Router D would never be a feasible successor no matter what the variance is. This decision is because the advertised distance of Router D is 25, which is greater than the Router E feasible distance of 20; therefore, to avoid a potential routing loop, Router D is not considered a feasible successor.

EIGRP Authentication

You can configure EIGRP neighbor authentication, also known as neighbor router authentication or route authentication, such that routers can participate in routing based on predefined passwords. By default, no authentication is used for EIGRP packets. EIGRP can be configured to use Message Digest Algorithm 5 (MD5) authentication.

When you configure neighbor authentication on a router, the router authenticates the source of each routing update packet that it receives. For EIGRP MD5 authentication, you must configure an authenticating key and a key ID on both the sending and the receiving router. The key is sometimes referred to as a password.

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 ID, which the router stores locally. The combination of the key ID and the interface that is associated with the message uniquely identifies the MD5 authentication key in use.

EIGRP enables you to manage keys by using key chains. Each key definition within the key chain can specify a time interval for which that key is activated (its lifetime). Then, during the lifetime of a given key, routing update packets are sent with this activated key. 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 it uses the first valid key that it encounters.

Keys cannot be used during time periods for which they are not activated. Therefore, it is recommended that for a given key chain, key activation times overlap to avoid any period of time for which no key is activated. If a time exists during which no key is activated, neighbor authentication cannot occur, and therefore, routing updates fail.

NOTE The routers must know the correct time to rotate through keys in synchronization with the other participating routers. This ensures that all the routers are using the same key at the same moment.

Creating a Key Chain

Perform the following steps to create a key chain:

Step 1 Enter the **key chain** command to enter the configuration mode for the key chain. The value provided for the *name-of-chain* parameter for the **key chain** command indicates the name of the authentication key chain from which a key is to be obtained.

Step 2 Use the **key** command to identify a key ID to use, and enter configuration mode for that key. The value provided for the *key-id* parameter of the **key** command indicates the ID number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key ID numbers need not be consecutive.

Step 3 Use the **key-string** command to identify the key string (password) for this key. The value provided for the *text* parameter of the **key-string** command indicates the authentication string that is to be used to authenticate sent and received EIGRP packets. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters. The first character cannot be a number, and the string is case sensitive.

Step 4 Optionally, use **accept-lifetime** to specify the time during which this key is accepted for use on received packets. If you do not enter an **accept-lifetime** command, the time is infinite. Table 5-7 describes the **accept-lifetime** command parameters.

Table 5-7 **accept-lifetime** *Parameters*

Parameter	Description
start-time	Beginning time that the key that is specified by the **key** command is valid for use on received packets. The syntax can be either of the following: hh:mm:ss month date year hh:mm:ss date month year where *hh*: Hours *mm*: Minutes *ss*: Seconds *month*: First three letters of the name of the month *date*: Date (1–31) *year*: Year (four digits) The default start time. The earliest acceptable date is January 1, 1993.
infinite	The key is valid for use on received packets from the *start-time* value on, with no end time.
end-time	The key is valid for use on received packets from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is infinite.
seconds	Length of time (in seconds) that the key is valid for use on received packets. The range is from 1 to 2147483646.

Step 5 Optionally, specify the time during which this key can be used for sending packets using the **send-lifetime** command. If you do not enter a **send-lifetime** command, the time is infinite. Table 5-8 describes the **send-lifetime** command parameters.

Table 5-8 **send-lifetime** *Parameters*

Parameter	Description
start-time	Beginning time that the key specified by the **key** command is valid to be used for sending packets. The syntax can be either of the following: *hh:mm:ss month date year* *hh:mm:ss date month year* where *hh*: Hours *mm*: Minutes *ss*: Seconds *month*: First three letters of the name of the month *date*: Date (1–31) *year*: Year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	The key is valid to be used for sending packets from the *start-time* value on.
end-time	The key is valid to be used for sending packets from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is infinite.
seconds	Length of time (in seconds) that the key is valid to be used for sending packets. The range is from 1 to 2147483646.

NOTE If the **service password-encryption** command is not used when you are implementing EIGRP authentication, the key string is stored as plain text in the router configuration. If you configure the **service password-encryption** command, the key string is stored and displayed in an encrypted form; when it is displayed, an encryption type of 7 is specified before the encrypted key string.

Configuring MD5 Authentication for EIGRP

To configure MD5 authentication for EIGRP, complete the following steps:

Step 1 Enter configuration mode for the interface on which you want to enable authentication.

Step 2 Use the **ip authentication mode eigrp** *autonomous-system* **md5** command to specify that MD5 authentication is to be used for EIGRP packets. The value provided for the *autonomous-system* parameter of the **ip authentication mode eigrp md5** command indicates the EIGRP AS number in which authentication is to be used.

Step 3 Use the **ip authentication key-chain eigrp** *autonomous-system name-of-chain* command to specify which key chain to use for the authentication of EIGRP packets. Table 5-9 describes the parameters for this command.

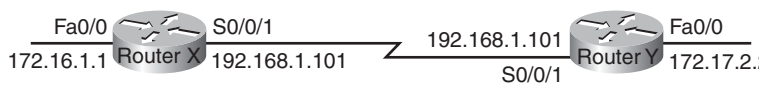
Table 5-9 **ip authentication key-chain eigrp** *Parameters*

Parameter	Description
autonomous-system	The EIGRP AS number in which authentication is to be used
name-of-chain	The name of the authentication key chain from which a key is to be obtained

Example: MD5 Authentication Configuration

Figure 5-7 shows an example network used for the configuration of EIGRP MD5 authentication for Router X in Example 5-6.

Figure 5-7 *Network Topology for EIGRP MD5 Configuration Example*



Example 5-6 *Configuring EIGRP MD5 Authentication on Router X*

```
RouterX
<output omitted>
key chain RouterXchain
 key 1
  key-string firstkey
  accept-lifetime 04:00:00 Jan 1 2006 infinite
  send-lifetime 04:00:00 Jan 1 2006 04:01:00 Jan 1 2006
 key 2
  key-string secondkey
  accept-lifetime 04:00:00 Jan 1 2006 infinite
```

Example 5-6 *Configuring EIGRP MD5 Authentication on Router X (Continued)*

```
  send-lifetime 04:00:00 Jan 1 2006 infinite
<output omitted>
!
interface Serial0/0/1
 bandwidth 64
 ip address 192.168.1.101 255.255.255.224
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 RouterXchain
```

MD5 authentication is configured on the Serial 0/0/1 interface with the **ip authentication mode eigrp 100 md5** command. The **ip authentication key-chain eigrp 100 RouterXchain** command specifies that the key chain RouterXchain is to be used for EIGRP AS 100.

The **key chain RouterXchain** command enters configuration mode for the RouterXchain key chain. Two keys are defined. Key 1 is set to "first key" with the **key-string firstkey** command. This key is acceptable for use on packets that are received by Router X from 4:00 a.m. (0400) on January 1, 2006, onward, as specified in the **accept-lifetime 04:00:00 Jan 1 2006 infinite** command. However, the **send-lifetime 04:00:00 Jan 1 2006 04:01:00 Jan 1 2006** command specifies that this key is valid for use only when packets are sent for one minute on January 1, 2006; afterward, it is no longer valid for use in sending packets.

Key 2 is set to "second key" with the **key-string secondkey** command. This key is acceptable for use on packets that are received by Router X from 4:00 a.m. (0400) on January 1, 2006, onward, as specified in the **accept-lifetime 04:00:00 Jan 1 2006 infinite** command. This key can also be used when packets are sent from 4:00 a.m. (0400) on January 1, 2006, onward, as specified in the **send-lifetime 04:00:00 Jan 1 2006 infinite** command.

Therefore, Router X accepts and attempts to verify the MD5 digest of any EIGRP packets with a key ID equal to 1. Router X will also accept a packet with a key ID equal to 2. All other MD5 packets are dropped. Router X sends all EIGRP packets using key 2 because key 1 is no longer valid for use in sending packets.

Example 5-7 shows the configuration of EIGRP MD5 authentication for Router Y in Figure 5-7.

Example 5-7 *Configuring EIGRP MD5 Authentication on Router Y*

```
RouterY
<output omitted>
key chain RouterYchain
 key 1
  key-string firstkey
  accept-lifetime 04:00:00 Jan 1 2006 infinite
  send-lifetime 04:00:00 Jan 1 2006 infinite
```

continues

Example 5-7 *Configuring EIGRP MD5 Authentication on Router Y (Continued)*

```
 key 2
  key-string secondkey
  accept-lifetime 04:00:00 Jan 1 2006 infinite
  send-lifetime 04:00:00 Jan 1 2006 infinite
<output omitted>
!
interface Serial0/0/1
 bandwidth 64
 ip address 192.168.1.102 255.255.255.224
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 RouterYchain
```

MD5 authentication is configured on the Serial 0/0/1 interface with the **ip authentication mode eigrp 100 md5** command. The **ip authentication key-chain eigrp 100 RouterYchain** command specifies that the key chain RouterYchain is to be used for EIGRP AS 100.

The **key chain RouterYchain** command enters configuration mode for the RouterYchain key chain. Two keys are defined. Key 1 is set to "first key" with the **key-string firstkey** command. This key is acceptable for use on packets that are received by Router Y from 4:00 a.m. (0400) on January 1, 2006, onward, as specified in the **accept-lifetime 04:00:00 Jan 1 2006 infinite** command. This key can also be used when packets are sent from 4:00 a.m. (0400) on January 1, 2006, onward, as specified in the **send-lifetime 04:00:00 Jan 1 2006 infinite** command.

Key 2 is set to "second key" with the **key-string secondkey** command. This key is acceptable for use on packets that are received by Router Y from 4:00 a.m. (0400) on January 1, 2006, onward, as specified in the **accept-lifetime 04:00:00 Jan 1 2006 infinite** command. This key can also be used when packets are sent from 4:00 a.m. (0400) on January 1, 2006, onward, as specified in the **send-lifetime 04:00:00 Jan 1 2006 infinite** command.

Therefore, Router Y accepts and attempts to verify the MD5 digest of any EIGRP packets with a key ID equal to 1 or 2. Router Y uses key 1 to send all EIGRP packets because it is the first valid key in the key chain.

Verifying MD5 Authentication

Example 5-8 shows the output of the **show ip eigrp neighbors** and **show ip route** commands on Router X.

Example 5-8 *Verifying EIGRP MD5 Authentication on Router X*

```
RouterX# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.1.102           Se0/0/1           12 00:03:10   17  2280  0  14

RouterX# show ip route
<output omitted>
Gateway of last resort is not set
D    172.17.0.0/16 [90/40514560] via 192.168.1.102, 00:02:22, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:31:31, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.96/27 is directly connected, Serial0/0/1
D       192.168.1.0/24 is a summary, 00:31:31, Null0

RouterX# ping 172.17.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/16 ms
```

The fact that the neighbor table shows the IP address of Router Y indicates that the two routers have successfully formed an EIGRP adjacency. The routing table verifies that the 172.17.0.0 network has been learned through EIGRP over the serial connection. Therefore, the MD5 authentication for EIGRP must have been successful between Router X and Router Y.

The results of a ping to the Router Y FastEthernet interface address are also displayed to illustrate that the link is working.

Summary of Implementing EIGRP

The following summarizes the key points that were discussed in the previous sections:

- EIGRP is a classless, advanced distance vector routing protocol that runs the DUAL algorithm.
- EIGRP requires you to configure an autonomous system number that must match on all routers to exchange routes.
- EIGRP is capable of load balancing across unequal-cost paths.
- EIGRP supports MD5 authentication to protect against unauthorized, rogue routers entering your network.

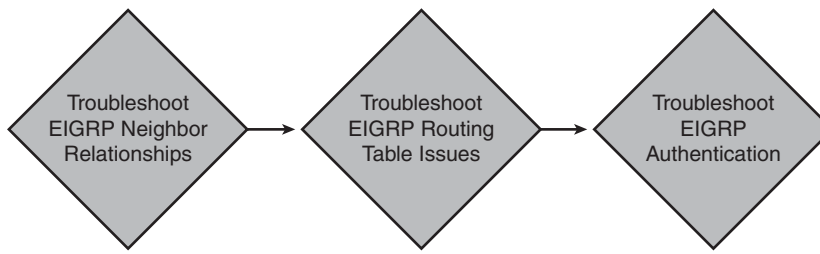
Troubleshooting EIGRP

As an advanced distance vector routing protocol, EIGRP scales well with a growing network. However, this scalability introduces complexity in design, configuration, and maintenance. This section introduces some of the common issues surrounding an EIGRP network and a flowchart approach to troubleshooting these issues.

Components of Troubleshooting EIGRP

When troubleshooting any network protocol, it is important to follow a defined flow or methodology. The main aspect of troubleshooting routing protocols involves ensuring that communication exists between the routers. The following sections describe the basic components of troubleshooting a network that is running EIGRP. Figure 5-8 shows an example of the flow used for diagnosing EIGRP problems.

Figure 5-8 *EIGRP Troubleshooting*



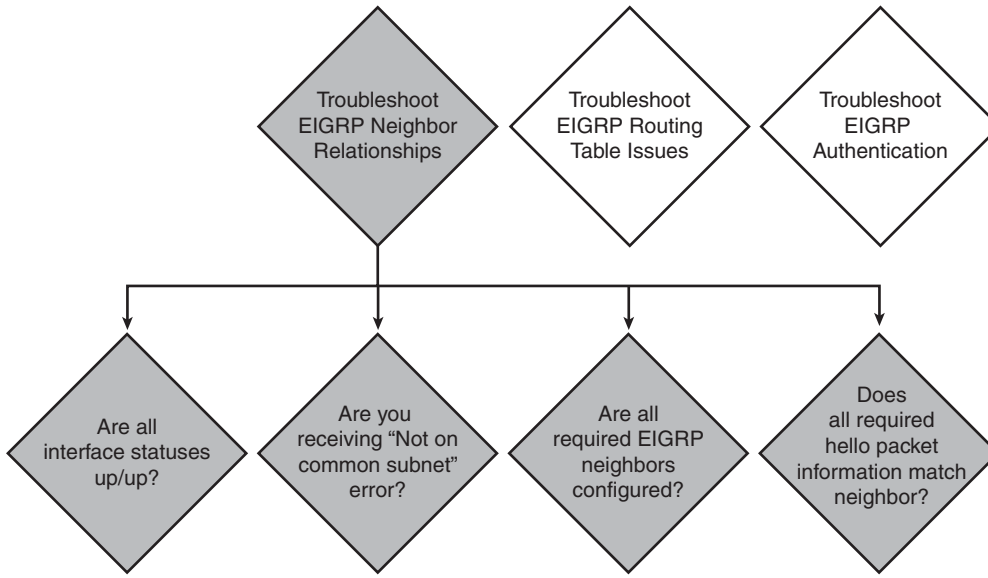
The major components of EIGRP troubleshooting include the following items:

- EIGRP neighbor relationships
- EIGRP routes in the routing table
- EIGRP authentication

Troubleshooting EIGRP Neighbor Relationships

The first step in the flow is to troubleshoot neighbor relationships. Figure 5-9 shows the steps for troubleshooting these issues.

Figure 5-9 *Troubleshooting EIGRP Neighbor Issues*



Example 5-9 shows output from the **show ip eigrp neighbors** command, which indicates that a successful neighbor relationship exists with two routers.

Example 5-9 *Confirming EIGRP Neighbor Relationships*

```
RouterX# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface       Hold Uptime   SRTT  RTO  Q   Seq
                                    (sec)         (ms)       Cnt Num
1   10.23.23.2      Se0/0/1         13 00:02:26   29    2280 0   15
0   10.140.1.1      Se0/0/0         10 00:28:26   24    2280 0   25
```

For EIGRP routers to form a neighbor relationship, both routers must share a directly connected IP subnet. A log message that displays that EIGRP neighbors are "not on common subnet" indicates that an improper IP address exists on one of the two EIGRP neighbor interfaces. Use the **show interface** *interface* command to verify the IP addresses.

In the output in Example 5-10, the interface address is 10.2.2.3/24.

Example 5-10 *Confirming EIGRP Neighbor IP Address*

```
RouterX# show ip interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.2.2.3/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
```

The **network** command that is configured under the EIGRP routing process indicates which router interfaces will participate in EIGRP. The "Routing for Networks" section of the **show ip protocols** command indicates that the networks have been configured; any interfaces in those networks participate in EIGRP. In the output of Example 5-11, EIGRP is running on any interfaces that have an IP address on the 10.0.0.0 and 192.168.1.0 networks.

Example 5-11 *Confirming Router Interface Participation in EIGRP Routing*

```
RouterX# show ip protocols
Routing Protocol is "eigrp 100"
  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
  Redistributing: eigrp 100
--output omitted --
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:01:08
    10.140.1.1            90      00:01:08
  Distance: internal 90 external 170
```

The **show ip eigrp interfaces** command can quickly indicate on which interfaces EIGRP is enabled and show how many neighbors can be found on each interface. In the output in

Example 5-12, no peers currently exist on the FastEthernet 0/0 interface, and one peer exists on the Serial 0/0/0 interface.

Example 5-12 *Confirming EIGRP Status and Neighbors on an Interface*

```
RouterX# show ip eigrp interfaces
IP-EIGRP interfaces for process 100

              Xmit Queue   Mean   Pacing Time   Multicast    Pending
Int    Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0    0        0/0         0       0/1            0           0
Se0/0/0  1        0/0        38      10/380        552           0
```

EIGRP routers create a neighbor relationship by exchanging hello packets. Certain fields in the hello packets must match before an EIGRP neighbor relationship is established:

- EIGRP autonomous system (AS) number
- EIGRP K values

> **NOTE** EIGRP K values are used in the EIGRP best-path selection process and are discussed in the Cisco CCNP curriculum.

You can use the **debug eigrp packets** command to troubleshoot when hello packet information does not match. In Example 5-13, a K value mismatch exists.

Example 5-13 *Verifying EIGRP Hello Packet Mismatches*

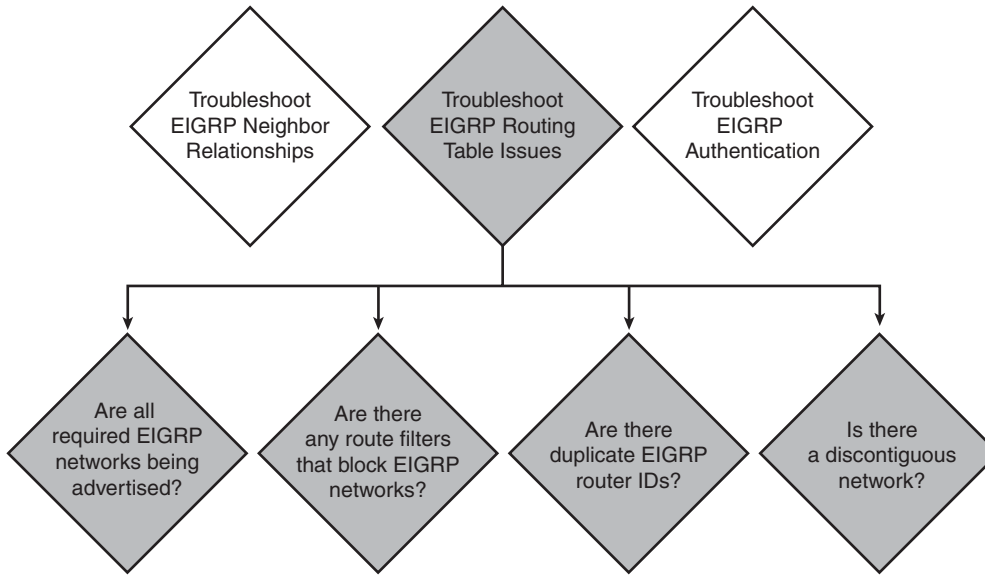
```
RouterX# debug eigrp packets

Mismatched adjacency values
01:39:13: EIGRP: Received HELLO on Serial0/0 nbr 10.1.2.2
01:39:13:AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
01:39:13:        K-value mismatch
```

Troubleshooting EIGRP Routing Tables

If the neighbor relationships are established, routes can be exchanged. If they are not being exchanged, the next step is to troubleshoot EIGRP routing table issues. Figure 5-10 shows the steps involved in troubleshooting these problems.

Figure 5-10 *Troubleshooting EIGRP Routing Tables*



EIGRP routes that appear with a "D" in the routing table indicate that they are intra-AS routes, and those with "D EX" indicate that they are external AS routes. No EIGRP routes in the routing table can indicate that a Layer 1 or 2 issue or an EIGRP neighbor problem exists.

In the output in Example 5-14, the 172.16.31.0/24 network is an intra-AS route, and 10.3.3.0/24 is a route that was redistributed into EIGRP.

Example 5-14 *Confirming EIGRP Intra-AS and Redistributed Routes*

```
RouterX# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.31.0/24 [90/40640000] via 10.140.1.1, 00:01:09, Serial0/0/0
O       172.16.31.100/32 [110/1563] via 10.140.1.1, 00:26:55, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.23.23.0/24 is directly connected, Serial0/0/1
D EX      10.3.3.0/24 [170/40514560] via 10.23.23.2, 00:01:09, Serial0/0/1
C       10.2.2.0/24 is directly connected, FastEthernet0/0
```

The **show ip eigrp topology** command displays the EIGRP router ID. The EIGRP router ID comes from the highest IP address assigned to a loopback interface. If no loopback interfaces are configured, the highest IP address assigned to any other active interface is chosen as the router ID. No two EIGRP routers can have the same EIGRP router ID. If they do, you will experience problems exchanging routes between the two routers with equal router IDs.

In the output in Example 5-15, the router ID is 192.168.1.65.

Example 5-15 *Displaying EIGRP Router IDs*

```
RouterX# show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(192.168.1.65)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.1.1.0/24, 1 successors, FD is 40514560
        via 10.140.1.1 (40514560/28160), Serial0/0/0
P 10.2.2.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 10.3.3.0/24, 1 successors, FD is 40514560
        via 10.23.23.2 (40514560/28160), Serial0/0/1
P 10.23.23.0/24, 1 successors, FD is 40512000
        via Connected, Serial0/0/1
P 192.168.1.64/28, 1 successors, FD is 128256
        via Connected, Loopback0
P 192.168.1.0/24, 1 successors, FD is 40640000
        via 10.23.23.2 (40640000/128256), Serial0/0/1
P 10.140.2.0/24, 2 successors, FD is 41024000
        via 10.23.23.2 (41024000/40512000), Serial0/0/1
        via 10.140.1.1 (41024000/40512000), Serial0/0/0
P 10.140.1.0/24, 1 successors, FD is 40512000
        via Connected, Serial0/0/0
P 172.16.31.0/24, 1 successors, FD is 40640000
```

EIGRP routes that are found in the topology table but not in the routing table can indicate an issue that requires help from Cisco Technical Assistance Center (TAC) to diagnose the problem.

Route filtering enables routes to be filtered from an EIGRP routing advertisement as they come in from a neighbor or as they are sent out to a neighbor. These filters can cause routes to be missing from the routing table. The **show ip protocols** command shows whether any filter lists are applied to EIGRP.

NOTE Filtering routing information is covered in the CCNP course materials.

By default, EIGRP is classful and performs automatic network summarization. Automatic network summarization causes connectivity issues in discontiguous networks. The **show ip protocols** command confirms whether automatic network summarization is in effect.

In the sample output in Example 5-16, no filter lists are applied to EIGRP AS 100, and automatic network summarization is in effect.

Example 5-16 *Confirming EIGRP Automatic Network Summarization*

```
RouterX# show ip protocols
Routing Protocol is "eigrp 100"
  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
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.1.0/24 for FastEthernet0/0, Serial0/0/0, Serial0/0/1
      Summarizing with metric 128256
    10.0.0.0/8 for Loopback0
      Summarizing with metric 28160
  Maximum path: 4
```

Troubleshooting EIGRP Authentication

The last step in the flowchart in Figure 5-8 is to troubleshoot EIGRP authentication problems, if configured. This is accomplished by verifying that EIGRP authentication is successful.

Example: Successful MD5 Authentication

The output of the **debug eigrp packets** command on Router X, shown in Example 5-17, illustrates that Router X is receiving EIGRP packets with MD5 authentication and a key ID equal to 1 from Router Y.

Example 5-17 *Confirming MD5 Authentication on Router X*

```
RouterX# debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
*Jan 21 16:38:51.745: EIGRP: received packet with MD5 authentication, key id = 1
*Jan 21 16:38:51.745: EIGRP: Received HELLO on Serial0/0/1 nbr 192.168.1.102
*Jan 21 16:38:51.745:   AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
  un/rely 0/0
```

Similarly, the output of the **debug eigrp packets** command on Router Y, shown in Example 5-18, illustrates that Router Y is receiving EIGRP packets with MD5 authentication and a key ID equal to 2 from Router X.

Example 5-18 *Confirming MD5 Authentication on Router Y*

```
RouterY# debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)
RouterY#
*Jan 21 16:38:38.321: EIGRP: received packet with MD5 authentication, key id = 2
*Jan 21 16:38:38.321: EIGRP: Received HELLO on Serial0/0/1 nbr 192.168.1.101
*Jan 21 16:38:38.321:   AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
  un/rely 0/0
```

Example: Troubleshooting MD5 Authentication Problems

In the example, the key string for key 2 of Router X, the one that is used when EIGRP packets are sent, is changed to be different from the key string that Router Y is expecting.

The output of the **debug eigrp packets** command on Router Y, shown in Example 5-19, illustrates that Router Y is receiving EIGRP packets with MD5 authentication and a key ID equal to 2 from Router X, but that an authentication mismatch exists. The EIGRP packets from Router X are ignored, and the neighbor relationship is declared to be down. The output of the **show ip eigrp neighbors** command should confirm that Router Y has no EIGRP neighbors.

Example 5-19 *MD5 Authentication Mismatch*

```
RouterY# debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
RouterY#
*Jan 21 16:50:18.749: EIGRP: pkt key id = 2, authentication mismatch
*Jan 21 16:50:18.749: EIGRP: Serial0/0/1: ignored packet from 192.168.1.101, opc
ode = 5 (invalid authentication)
*Jan 21 16:50:18.749: EIGRP: Dropping peer, invalid authentication
*Jan 21 16:50:18.749: EIGRP: Sending HELLO on Serial0/0/1
*Jan 21 16:50:18.749:   AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
*Jan 21 16:50:18.753: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.1.101
 (Serial0/0/1) is down: Auth failure

RouterY# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
RouterY#
```

The two routers keep trying to reestablish their neighbor relationship. Because of the different keys that are used by each router in this scenario, Router X authenticates the hello messages that are sent by Router Y using key 1. However, when Router X sends a hello message back to Router Y using key 2, an authentication mismatch will occur. From the perspective of Router X, the relationship appears to be up for a while, but then it times out, as illustrated by the messages that were received on Router X, shown in Example 5-20. The output of the **show ip eigrp neighbors** command on Router X also illustrates that Router X does have Router Y in its neighbor table for a short time.

Example 5-20 *Confirming MD5 Authentication*

```
RouterX# debug eigrp packets
*Jan 21 16:54:09.821: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.1.102 (Serial0/
  0/1) is down: retry limit exceeded
*Jan 21 16:54:11.745: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.1.102 (Serial0/
  0/1) is up: new adjacency
RouterX# show ip eigrp neighbors
H Address   Interface Hold Uptime SRTT RTO Q Seq
                              (sec)          (ms)       Cnt Num
0   192.168.1.102  Se0/0/1       13 00:00:38    1   5000  1  0
```

Summary of Troubleshooting EIGRP

The following summarizes the key points that were discussed in this section:

- Troubleshooting EIGRP includes several aspects, such as resolving neighbor relationships, routing table issues, and authentication problems.
- Issues that can cause EIGRP neighbor problems include incorrect network commands and hello packet information mismatches. Use the **show ip eigrp neighbors** command to help troubleshoot these issues.
- Missing EIGRP routes from the routing table can be because of route filtering or automatic summarization in discontiguous networks. Use the **show ip route** command to help troubleshoot these issues.
- The **debug eigrp packets** command can help you troubleshoot MD5 authentication problems.

Chapter Summary

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco routing protocol that is designed to address the shortcomings of both distance vector and link-state routing protocols. This chapter expanded on the underlying technologies within EIGRP, including the path selection process, changes in topology, load balancing, authentication, and troubleshooting common problems.

The following summarizes the key points that were discussed in this chapter:

- EIGRP is a classless routing protocol that supports VLSM.
- Path selection is based on several factors.
- EIGRP keeps a next-best alternative path, called a feasible successor, for fast convergence.
- EIGRP supports unequal-cost load balancing.
- EIGRP uses MD5 authentication for router authenticity.
- Troubleshooting EIGRP requires resolving link, neighbor, redistribution, and routing issues.
- The following commands help you troubleshoot EIGRP issues: **show ip eigrp neighbor**, **show ip eigrp topology**, **show ip eigrp interface**, and **show ip route**.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers and solutions are found in the appendix, "Answers to Chapter Review Questions."

1. How do you minimize the bandwidth requirement for EIGRP packets?
   a. By propagating only data packets
   b. By propagating only hello packets
   c. By propagating only routing table changes and hello packets
   d. By propagating the entire routing table only to those routers that are affected by a topology change
2. Which command correctly specifies that network 10.0.0.0 is directly connected to a router that is running EIGRP?
   a. Router(config)# **network 10.0.0.0**
   b. Router(config)# **router eigrp 10.0.0.0**
   c. Router(config-router)# **network 10.0.0.0**
   d. Router(config-router)# **router eigrp 10.0.0.0**
3. Which command displays the amount of time since the router heard from an EIGRP neighbor?
   a. **show ip eigrp traffic**
   b. **show ip eigrp topology**
   c. **show ip eigrp interfaces**
   d. **show ip eigrp neighbors**

4. Which command must you configure for EIGRP to pass the subnet mask with the route?
   a. **ip classless**
   b. **no auto-summary**
   c. **no summary**
   d. **ip subnet vlsm**
5. Which command displays whether route filtering has been enabled?
   a. **show interface**
   b. **show access-list**
   c. **show ip protocols**
   d. **show route-filter**
6. Which form of authentication does EIGRP support?
   a. Plain text
   b. 3DES
   c. MD5
   d. Both A and C
7. What does the EIGRP message "neighbor not on common subnet" mean?
   a. Duplicate EIGRP router IDs exist.
   b. The two adjacent neighbor interfaces do not have addresses in the same IP network.
   c. The MTU sizes on the two adjacent neighbor routers do not match.

Index

SYMBOLS

NUMBERS

A

B

C

D

E

F

G - H

I

J - K - L

M

N

O

P

Q - R

S

T

U - V

W - X - Y - Z