Interconnecting Cisco Network Devices, Part 2 (ICND2)
Foundation Learning Guide

FREE SAMPLE CHAPTER
SHARE WITH OTHERS
Interconnecting Cisco Network Devices, Part 2 (ICND2)


John Tiso

John Tiso

Copyright © 2014 Cisco Systems, Inc.

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

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing September 2013

Library of Congress Control Number: 2013946147

Warning and Disclaimer

This book is designed to provide information about interconnecting Cisco network devices, the ICND2 portion of the CCNA exam. 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 author, 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.
About the Author

John Tiso, CCIE #5162, holds a variety of industry certifications in addition to his Cisco CCIE. These include the Cisco CCDP, Cisco CCNP-Voice, Cisco CCT, and several specializations from Cisco. He is a Microsoft MCSE and also holds certifications from CompTIA, Nortel Networks, Novell, Sun Microsystems, IBM, and HP.

John has a Graduate Citation in Strategic Management from Harvard University and a B.S. degree from Adelphi University. His writing has been published in a variety of industry journals and by Cisco Press. He has served as a technical editor for McGraw-Hill and Cisco Press. John is a past Esteemed Speaker for Cisco Networkers (Live!) and was a speaker at the National CIPTUG Conference. He has been an expert on Cisco’s “Ask the Expert” NetPro forum and a question developer for the CCIE program.

John's current role is as a senior engineer at a Cisco Partner. He has a quarter of a century experience in the technology industry, after deciding to stop carrying refrigerators in the family business. Prior to his current position, he held multiple roles while working at Cisco, including TAC Engineer, Systems Engineer, and Product Manager. While at Cisco, one of John’s last projects was as a member of the team that developed the recent updates to the CCNA program. Prior to joining Cisco, he was a lead architect and consultant for a Cisco Gold Partner.

John currently resides in Amherst, New Hampshire, with his wife Lauren and their three children, Kati, Nick, and Danny. John is a nine-time marathon finisher and also a Therapy Dog International certified handler of his therapy dog and running partner, Molly. He can be reached at johnt@jtiso.com.
About the Technical Reviewers

Marjan Bradeško has always practiced this principle: If you know something, if you experienced something, if you learned something—tell. That's exactly what he has done throughout his many years at NIL Ltd., and he continues to strive to do it today in his role of Content Development Manager.

Marjan was involved in learning services even prior to joining NIL in 1991. He came from the Faculty of Computer and Information Science at the University of Ljubljana, where he achieved his M.Sc. in computer science and was a teaching assistant. Soon after he joined NIL, the company became a Cisco Systems VAR, and Marjan's subsequent years are all “flavored” with Cisco. In all his various roles—from network engineer, consultant, or instructor to various management positions—Marjan's major goal has always been to educate, teach, and help people to achieve competencies in whatever they do. He has always been passionate about the importance of enthusiastic presentation of high-quality content to motivated people. He has long aided NIL employees in excelling at presentation skills and creating content to help NIL customers achieve competencies in IT and communications technologies. Marjan has also been heavily involved in promoting networking, Internet, cloud, and similar new technologies and publishing articles in numerous magazines.

Through his transitions from software engineer to his current position selling learning services as Content Development Manager, Marjan has gained broad knowledge and many competencies that he gladly shares with customers and coworkers. Marjan became a CCIE in 1995, stayed a CCIE for 16 years, and is now CCIE Emeritus. As a networking veteran, he has seen frequent technology reinventions, and he has had to learn and relearn repeatedly as innovative solutions have revolutionized the industry.

Marjan's passion for sharing his experiences is reflected in his private life as well. As an enthusiastic traveler and nature lover, especially of mountains, he has published many articles and books on nature and beautiful places of the world. In addition, he writes articles and books on presentation skills and sales, showing everyone that competencies are not given, but rather a merging of talent, learning, and hard work.

Diane Teare, CCNP, CCDP, PMP, is a professional in the networking, training, project management, and e-learning fields. She has more than 25 years of experience in designing, implementing, and troubleshooting network hardware and software, and has been involved in teaching, course design, and project management. She has extensive knowledge of network design and routing technologies, and is an instructor with one of the largest authorized Cisco Learning Partners. She was the director of e-learning for the same company, where she was responsible for planning and supporting all the company’s e-learning offerings in Canada, including Cisco courses. Diane has a bachelor’s degree in applied science in electrical engineering and a master’s degree in applied science in management science.
Dedication

To everyone who helped me find my way back.
Acknowledgments

I’d like to thank the crew at Cisco Press. This includes Brett Bartow, Chris Cleveland, Marianne Bartow (who was my savior, yet again), and Mandie Frank. Your support and sticking with me through the difficulties and challenges I faced during this project meant a lot to me, and was much appreciated. Thank you.

I’d like to thank the technical editors, Marjan and Diane. I’m happy I had the opportunity to meet you in person before I left Cisco and ask you to work on this project. I found your experience with the ICND2 course, your industry experience, and your diligent attention to detail invaluable. I really made you earn your money on this one! Thanks so much!

Lauren, Danny, Nick, and Kati; Thank you for bearing with me under both our normal day-to-day life, as well as when I had to disappear to work on this project. I’d also like to thank Lauren for her photography on several of the photos as well.

I’d also like to thank you, the reader and certification candidate, for your selection of this book.

For everyone else who I did not directly mention, thanks for everything. I keep the words of “The Boss” in my head, “It ain't no sin to be glad you're alive.”
Contents at a Glance

Chapter 1  Implementing Scalable Medium-Sized Networks  1
Chapter 2  Troubleshooting Basic Connectivity  47
Chapter 3  Implementing an EIGRP Solution  91
Chapter 4  Implementing a Scalable Multiarea Network with OSPF  143
Chapter 5  Understanding WAN Technologies  185
Chapter 6  Network Device Management  269
Chapter 7  Advanced Troubleshooting  339
Appendix A  Answers to Chapter Review Questions  363
Appendix B  Basic L3VPN MPLS Configuration and Verification  369

Glossary of Key Terms  375
Index  403
Contents

Introduction xviii

Chapter 1 Implementing Scalable Medium-Sized Networks 1

Understanding and Troubleshooting VLANs and VLAN Trunking 2

VLAN Overview 2

Trunk Operation 6

Configuring Trunks 7

Dynamic Trunking Protocol 8

VLAN Troubleshooting 9

Trunk Troubleshooting 10

Building Redundant Switch Topologies 11

Understanding Redundant Topologies 12

BPDU Breakdown 15

STP Types Defined 20

Per-VLAN Spanning Tree Plus 21

Analyzing and Reviewing STP Topology and Operation 24

Examining Spanning-Tree Failures 26

STP Features: PortFast, BPDU Guard, Root Guard, UplinkFast, and BackboneFast 28

Improving Redundancy and Increasing Bandwidth with EtherChannel 29

EtherChannel Protocols 31

Port Aggregation Protocol 31

Link Aggregation Control Protocol 32

Configuring EtherChannel 33

Checking EtherChannel Operation 34

Understanding Default Gateway Redundancy 36

Hot Standby Router Protocol 37

HSRP Interface Tracking 38

HSRP Load Balancing 39

HSRP in Service Deployments 39

HSRP in IPv6 40

Gateway Load-Balancing Protocol 40

Chapter Summary 42

Review Questions 42
Chapter 2  Troubleshooting Basic Connectivity  47

Troubleshooting IPv4 Basic Connectivity  48
  Components of End-to-End IPv4 Troubleshooting  48
  Verification of Connectivity  51
Cisco Discovery Protocol  58
Verification of Physical Connectivity Issues  60
Identification of Current and Desired Path  63
Default Gateway Issues  66
Name Resolution Issues  68
ACL Issues  71
Understanding Networking in Virtualized Computing Environments  72

Troubleshooting IPv6 Network Connectivity  75
  Understanding IPv6 Addressing  75
IPv6 Unicast Addresses  76
  Components of Troubleshooting End-to-End IPv6 Connectivity  78
Verification of End-to-End IPv6 Connectivity  79
Neighbor Discovery in IPv6  80
Identification of Current and Desired IPv6 Path  82
Default Gateway Issues in IPv6  82
Name Resolution Issues in IPv6  83
ACL Issues in IPv6  84
IPv6 in a Virtual Environment  86

A Last Note on Troubleshooting  86
Chapter Summary  88
Review Questions  88

Chapter 3  Implementing an EIGRP Solution  91

Dynamic Routing Review  92
  Routing  92
  Routing Domains  92
  Classification of Routing Protocols  93
  Classful Routing Versus Classless Routing  94
  Administrative Distance  95
EIGRP Features and Function  98
  EIGRP Packet Types  100
  EIGRP Path Selection  101
Understanding the EIGRP Metric  103
Chapter 4  Implementing a Scalable Multiarea Network with OSPF  143

Understanding OSPF  143

- Link-State Routing Protocol Overview  144
- Link-State Routing Protocol Data Structures  145
- Understanding Metrics in OSPF  146
- Establishment of OSPF Neighbor Adjacencies  147
- Building a Link-State Database  149
- OSPF Area Structure  150
- OSPF Area and Router Types  150
- Link-State Advertisements  153

Multiarea OSPF IPv4 Implementation  154

- Single-Area vs. Multiarea OSPF  155
- Stub Areas, Not So Stubby Areas, and Totally Stub Areas  155
Planning for the Implementation of OSPF  158
Multiarea OSPF Configuration  158
Multiarea OSPF Verification  160
Troubleshooting Multiarea OSPF  162
OSPF Neighbor States  162
Components of Troubleshooting OSPF  166
Troubleshooting OSPF Neighbor Issues  168
Troubleshooting OSPF Routing Table Issues  172
Troubleshooting OSPF Path Selection  174
Examining OSPFv3  176
OSPFv3 Key Characteristics  176
OSPFv3 LSAs  177
Configuring OSPFv3  178
OSPFv3 Verification  179
Chapter Summary  180
Review Questions  181

Chapter 5  Understanding WAN Technologies  185
Understanding WAN Technologies  186
  WAN Architecture  188
  Hub-and-Spoke Networks  188
  Partial-Mesh Networks  189
  Full-Mesh Networks  189
  Point-to-Point Networks  191
  WAN Devices  192
  Serial WAN Cabling  195
  WAN Layer 2 Protocols  197
  Other WAN Protocols  199
  Integrated Services Digital Network  199
  X.25  199
  Multiprotocol Label Switching  200
  Service Provider Demarcation Points  200
  T1/E1  200
  DSL Termination  201
  Cable Termination  202
  Other WAN Termination  203
  WAN Link Options  203
  Private WAN Connection Options  204
Chapter 6  Network Device Management  269

Configuring Network Devices to Support Network Management  270

SNMP Versions  270

Obtaining Data from an SNMP Agent  271

Monitoring Polling Data in SNMP  272

Monitoring TRAPs in SNMP  273

Sending Data to an SNMP Agent  274

SNMP MIBs  275

Basic SNMP Configuration and Verification  276

Syslog Overview  279

Syslog Message Format  281

Syslog Configuration  281

NetFlow Overview  283

NetFlow Architecture  285

NetFlow Configuration  286

Verifying NetFlow Operation  287

Router Initialization and Configuration  288

Router Internal Component Review  289

ROM Functions  291

Router Power-Up Sequence  292

Configuration Register  293

Changing the Configuration Register  294

Locating the Cisco IOS Image to Load  295

Loading a Cisco IOS Image File  297

Selecting and Loading the Configuration  300

Cisco IOS File System and Devices  302

Managing Cisco IOS Images  305

Interpreting Cisco IOS Image Filenames  305

Creating a Cisco IOS Image Backup  306

Upgrading the Cisco IOS Image  308

Managing Device Configuration Files  311

Cisco IOS Password Recovery  313

Cisco IOS Licensing  315

Licensing Overview  315
Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the Cisco IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally, as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a `show` command).

- **Italics** indicates arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ]) indicate optional elements.

- Braces ({ }) indicate a required choice.

- Braces within brackets ([[ ]]) indicate a required choice within an optional element.
Introduction

The purpose of this book is to enable readers to obtain a higher level of foundational knowledge beyond the ICND1 books and course. This book provides numerous illustrations, examples, photographs, self-check questions, and additional background information for reinforcement of the information presented. I have drawn on real-world experience and examples for some of the information.

Cisco develops the career certifications, such as CCNA, to align to job roles. Cisco Press introduced the Foundation Learning Guide Series as a learning tool and a parallel resource for the instructor-led Cisco courses. This book is intended both to teach the fundamentals that a CCNA needs in their job role and to provide the knowledge required to pass the ICND2 exam (or the ICND2 components in the CCNA Composite exam).

In my last role at Cisco, I was involved in the development of the updates to the CCNA program. Based on this experience, I have included some fundamental information in this book that is not directly part of the current ICND2 or CCNA composite exams or the ICND2 instructor-led training (however, it may very well be included in subsequent updates to the CCNA). I included this information (that you will not find in any other CCNA book) to help create and support the foundation necessary for both the job role and to obtain the certification. Areas that I have included that are not necessarily part of the CCNA certification are: MPLS, virtualization, and advanced troubleshooting techniques such as information on IOS debugging.

Debugging is a useful skill for diagnosing network problems. It is also key to understanding how protocols and features work, by using debugging in a lab environment (examples of both uses are given in Chapter 7, “Advanced Troubleshooting”). Improper use of debugging can also cripple a network (also discussed in Chapter 7). Therefore, this type of supplemental knowledge helps support both the job role of a CCNA and the use of alternate techniques and technologies as a study tool.

If you are a certification candidate, I strongly suggest you check the exam blueprints on the Cisco Learning Network (https://learningnetwork.cisco.com/) before embarking on your studying adventure.

Thanks for selecting this book as part of your library, and all the best of luck in your quest for knowledge and certification.
**Who Should Read This Book?**

There are four primary audiences for this text:

- The network engineer who needs to review key technologies that are important in today’s networks
- The reader who is interested in learning about computer networking but might lack any previous experience in the subject
- The reader in the job role targeted for a CCNA who needs to obtain and update fundamental knowledge
- The reader who is interested in obtaining the Cisco CCNA certification

**How This Book Is Organized**

Certainly, this book may be read cover to cover. But it is designed to be flexible and to allow you to easily move between chapters and sections of chapters to cover only the material you need to learn or would like to revisit. If you do intend to read all of the chapters, the order in which they are presented is an excellent sequence.

Chapter 1: Implementing Scalable Medium Sized Networks. This chapter explores the basic foundational topics of internetworking, VLANs, EtherChannel, Spanning-Tree Protocol, and router redundancy (HSRP, VRRP, GLBP).

Chapter 2: Troubleshooting Basic Connectivity. Tools, techniques, and understanding basic error messaging and using host based and Cisco IOS Software are reviewed. IPv4, IPv6, and Virtualization are explored.

Chapter 3: Implementing an EIGRP Solution. EIGRP theory, operation, and troubleshooting for both IPv4 and IPv6 are discussed.

Chapter 4: Implementing a Scalable Multiarea Network with OSPF. The OSPF routing protocol is introduced. OSPF terminology, operation, configuration, and troubleshooting are explored.

Chapter 5: Understanding WAN technologies. WAN technologies are explored. This includes terminology, theory, configuration, and basic troubleshooting. VPNs are included as part of the chapter. This includes their comparison and integration with traditional WAN technology.

Chapter 6: Network Device Management. This chapter explores the various protocols such as SNMP, SYSLOG, and Cisco Flexible NetFlow. The architecture of the Cisco Integrated Service Routers is discussed. The management of configurations, Cisco IOS Software images, and licensing is explored.
Chapter 7: Advanced Troubleshooting. This chapter explores fundamental theory around advanced troubleshooting. It involves advanced diagnostics, Cisco IOS Software bugs, and Cisco IOS Debugging. The topics in this chapter are all directly outside the scope of the CCNA exam. However, understanding these topics will help the reader in both the job role as a CCNA and in exam preparation.

Appendix A: This appendix contains answers to the end of chapter questions.

Appendix B: This appendix contains information on very basic (customer side) configuration and troubleshooting of the MPLS WAN protocol. Again, the topics in this appendix are all directly outside the scope of the CCNA exam. However, understanding these topics will help the reader in both the job role as a CCNA and in exam preparation.

Glossary: Internetworking terms and acronyms are designed to assist the reader in the understanding of the text.
This page intentionally left blank
Chapter 3

Implementing an EIGRP Solution

This chapter contains the following sections:

- Dynamic Routing Review
- EIGRP Features and Function
- Troubleshooting EIGRP
- Implementing EIGRP for IPv6
- Chapter Summary
- Review Questions

EIGRP, Enhanced Interior Gateway Protocol, is an advanced distance vector routing protocol that was developed by Cisco over 20 years ago. It is suited for many different topologies and media. EIGRP scales well and provides extremely quick convergence times with minimal overhead. EIGRP performs in both well-designed networks and poorly designed networks. It is a popular choice for a routing protocol on Cisco devices. EIGRP did have a predecessor, Interior Gateway Protocol (IGRP), which is now obsolete and is not included in Cisco IOS 15.

EIGRP was historically a Cisco proprietary and closed protocol. However, as of this writing, Cisco is in the process of releasing the basic functions to the IETF as an RFC (Request For Comments, a standards document; see http://tools.ietf.org/html/draft-savage-eigrp-00).

This chapter begins with a review of dynamic routing. It then examines the operation, configuration, and troubleshooting of EIGRP for IPv4 and IPv6.
Chapter Objectives:
- Review key concepts for Dynamic Routing Protocols
- Understand how a Cisco Router populates its routing table
- Understand the features, operation, theory, and functions of EIGRP
- Configure and troubleshoot EIGRP for IPv6 and IPv4

Dynamic Routing Review
A dynamic routing protocol is a set of processes, algorithms, and messages that is used to exchange routing and reachability information within the internetwork. Without a dynamic routing protocol, all networks, except those connected directly with the router, must be statically defined. Dynamic routing protocols can react to changes in conditions in the network, such as failed links.

Routing
All routing protocols have the same purpose: to learn about remote networks and to quickly adapt whenever there is a change in the topology. The method that a routing protocol uses to accomplish this purpose depends upon the algorithm that it uses and the operational characteristics of the protocol. The performance of a dynamic routing protocol varies depending on the type of routing protocol.

Although routing protocols provide routers with up-to-date routing tables, there are costs that put additional demands on the memory and processing power of the router. First, the exchange of route information adds overhead that consumes network bandwidth. This overhead can be a problem, particularly for low-bandwidth links between routers. Second, after the router receives the route information, the routing protocol needs to process the information received. Therefore, routers that employ these protocols must have sufficient resources to implement the algorithms of the protocol and to perform timely packet routing and forwarding.

Routing Domains
An autonomous system (AS), otherwise known as a routing domain, is a collection of routers under a common administration. A typical example is an internal network of a company and its interconnection to the network of an ISP. The ISP and a company’s internal network are under different control. Therefore, they need a way to interconnect. Static routes are often used in this type of a scenario. However, what if there are multiple links between the company and the ISP? What if the company uses more than one ISP? Static routing protocols would not be suitable. To connect the entities, it is necessary to establish communication with the bodies under different administration. Another example would be a merger, acquisition, or development of a subsidiary that maintains its own IT resources. The networks may need to be connected, but they also may need to be main-
tained as separate entities. There must be a way to communicate between the two. The third example, which is intimated by the first, is the public Internet. Many different entities are interconnected here as well. Figure 3-1 is a representation of three autonomous systems, one for a private company and two ISPs.

![Figure 3-1](connection_of_three_distinct_autonomous_systems_as.png)

**Figure 3-1** *Connection of Three Distinct Autonomous Systems (AS)*

To accommodate these types of scenarios, two categories of routing protocols exist:

- **Interior Gateway Protocols (IGP):** These routing protocols are used to exchange routing information within an autonomous system. EIGRP, IS-IS (Intermediate System-to-Intermediate System) Protocol, RIP (Routing Information Protocol), and OSPF (Open Shortest Path First) Protocol are examples of IGPs.

- **Exterior Gateway Protocols (EGP):** These routing protocols are used to route between autonomous systems. BGP (Border Gateway Protocol) is the EGP of choice in networks today. The Exterior Gateway Protocol, designed in 1982, was the first EGP. It has since been deprecated in favor of BGP and is considered obsolete. BGP is the routing protocol used on the public Internet.

### Classification of Routing Protocols

EGPs and IGPs are further classified depending on how they are designed and operate. There are two categories of routing protocols:

- **Distance vector protocols:** The distance vector routing approach determines the direction (vector) and distance (hops) to any point in the internetwork. Some distance vector protocols periodically send complete routing tables to all of the connected neighbors. In large networks, these routing updates can become enormous, causing significant traffic on the links. This can also cause slow convergence, as the whole
routing table could be inconsistent due to network changes, such as a link down, between updates. RIP is an example of a protocol that sends out periodic updates.

Distance vector protocols use routers as signposts along the path to the final destination. The only information that a router knows about a remote network is the distance or metric to reach that network and which path or interface to use to get there. Distance vector routing protocols do not have an actual map of the network topology. EIGRP is another example of the distance vector routing protocol. However, unlike RIP, EIGRP does not send out full copies of the routing table once the initial setup occurs between two neighboring routers. EIGRP only sends updates when there is a change.

- **Link-state protocols:** The link-state approach, which uses the shortest path first (SPF) algorithm, creates an abstract of the exact topology of the entire internetwork, or at least of the partition in which the router is situated. Using a link-state routing protocol is like having a complete map of the network topology. Signposts along the way from the source to the destination are not necessary because all link-state routers are using an identical “map” of the network. A link-state router uses the link-state information to create a topology map and select the best path to all destination networks in the topology. Link-state protocols only send updates when there is a change in the network. BGP, OSPF, and IS-IS are examples of link-state routing protocols.

**Note** EIGRP was originally classified as a “hybrid” routing protocol, the combination of link state and distance vector. However, it is truly a rich-featured distance vector protocol. A major differentiator to support this is that EIGRP does not have a full picture of the topology in each node.

**Classful Routing Versus Classless Routing**

IP addresses are categorized in classes: A, B, and C. Classful routing protocols only recognize networks as directly connected by class. So, if a network is subnetted, there cannot be a classful boundary in between. In Figure 3-2, Network A cannot reach Network B using a classful routing protocol because they are separated by a different class network. The term for this scenario is *discontiguous subnets*.

Classful routing is a consequence when subnet masks are not disclosed in the routing advertisements that most distance vector routing protocols generate. When a classful routing protocol is used, all subnetworks of the same major network (Class A, B, or C) must use the same subnet mask, which is not necessarily a default major-class subnet mask. Routers that are running a classful routing protocol perform automatic route summarization across network boundaries. Classful routing has become somewhat obsolete because the classful model is rarely used on the Internet. Because IP address depletion problems occur on the Internet, most Internet blocks are subdivided using classless routing and variable-length subnet masks. You will most likely see classful address allocation inside private organizations that use private IP addresses as defined in RFC 1918 in conjunction with Network Address Translation (NAT) at AS borders.
Classless routing protocols can be considered second-generation protocols because they are designed to address some of the limitations of the earlier classful routing protocols. A serious limitation in a classful network environment is that the subnet mask is not exchanged during the routing update process, thus requiring the same subnet mask to be used on all subnetworks within the same major network. Another limitation of the classful approach is the need to automatically summarize to the classful network number at all major network boundaries. In the classless environment, the summarization process is controlled manually and can usually be invoked at any bit position within the address. Because subnet routes are propagated throughout the routing domain, manual summarization may be required to keep the size of the routing tables manageable. Classless routing protocols include BGP, RIPv2, EIGRP, OSPF, and IS-IS. Classful routing protocols include Cisco IGRP and RIPv1.

**Note**  
RFC 1918 defines the following networks for private use, meaning they are not routed on the public Internet: 10.0.0.0/8, 172.16.0.0/16–172.31.0.0/26, and 192.168.0.0/24–192.168.255.0/24. For more information on RFC 1918, see [http://tools.ietf.org/html/rfc1918](http://tools.ietf.org/html/rfc1918).

**Administrative Distance**  
Multiple routing protocols and static routes may be used at the same time. If there are several sources for routing information, including specific routing protocols, static routes, and even directly connected networks, an administrative distance value is used to rate the
trustworthiness of each routing information source. Cisco IOS Software uses the administrative distance feature to select the best path when it learns about the exact same destination network from two or more routing sources.

An administrative distance is an integer from 0 to 255. A routing protocol with a lower administrative distance is more trustworthy than one with a higher administrative distance. Table 3-1 displays the default administrative distances.

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Administrative Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directly connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route</td>
<td>1</td>
</tr>
<tr>
<td>eBGP (external BGP; between two different AS)</td>
<td>20</td>
</tr>
<tr>
<td>EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>RIP (both v1 and v2)</td>
<td>120</td>
</tr>
<tr>
<td>EIGRP External</td>
<td>170</td>
</tr>
<tr>
<td>iBGP (internal BGP, inside AS)</td>
<td>200</td>
</tr>
<tr>
<td>Unknown/untrusted source</td>
<td>255</td>
</tr>
</tbody>
</table>

Note There are other administrative distances, the discussion of which is beyond the scope of this text. See http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094195.shtml for more information.

As shown in the example in Figure 3-3, the router must deliver a packet from Network A to Network B. The router must choose between two routes. One is routed by EIGRP, and the other is routed by OSPF. Although the OSPF route appears to be the logical choice, given that it includes fewer hops to the destination network, the EIGRP route is identified as more trustworthy and is added to the routing table of the router.
A good way to detect which routing protocols are configured on the router is to execute `show ip protocols`. Example 3-1 gives output from a sample router running OSPF, EIGRP, and BGP. The command provides details regarding each routing protocol, including the administrative distance (Distance), values the routing protocol is using, and other features such as route filtering.

**Example 3-1  show ip protocols Command Output**

<table>
<thead>
<tr>
<th>Branch# show ip protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Protocol is &quot;eigrp 1&quot;</td>
</tr>
<tr>
<td>Outgoing update filter list for all interfaces is not set</td>
</tr>
<tr>
<td>Incoming update filter list for all interfaces is not set</td>
</tr>
<tr>
<td>Default networks flagged in outgoing updates</td>
</tr>
<tr>
<td>Default networks accepted from incoming updates</td>
</tr>
<tr>
<td>EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0</td>
</tr>
<tr>
<td>EIGRP maximum hopcount 100</td>
</tr>
<tr>
<td>EIGRP maximum metric variance 1</td>
</tr>
<tr>
<td>Redistributing: eigrp 1</td>
</tr>
<tr>
<td>EIGRP NSF-aware route hold timer is 240s</td>
</tr>
<tr>
<td>Automatic network summarization is in effect</td>
</tr>
<tr>
<td>Automatic address summarization:</td>
</tr>
<tr>
<td>192.200.200.0/24 for Loopback0, Loopback100</td>
</tr>
<tr>
<td>192.168.1.0/24 for Loopback0, Vlan1</td>
</tr>
<tr>
<td>172.16.0.0/16 for Loopback100, Vlan1</td>
</tr>
<tr>
<td>Summarizing with metric 128256</td>
</tr>
<tr>
<td>Maximum path: 4</td>
</tr>
<tr>
<td>Routing for Networks:</td>
</tr>
<tr>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Routing Information Sources:</td>
</tr>
<tr>
<td>Gateway Distance Last Update</td>
</tr>
<tr>
<td>(this router) 90 00:00:18</td>
</tr>
<tr>
<td>Distance: internal 90 external 170</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Routing Protocol is &quot;eigrp 100&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outgoing update filter list for all interfaces is not set</td>
</tr>
<tr>
<td>Incoming update filter list for all interfaces is not set</td>
</tr>
<tr>
<td>Default networks flagged in outgoing updates</td>
</tr>
<tr>
<td>Default networks accepted from incoming updates</td>
</tr>
<tr>
<td>EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0</td>
</tr>
<tr>
<td>EIGRP maximum hopcount 100</td>
</tr>
<tr>
<td>EIGRP maximum metric variance 1</td>
</tr>
<tr>
<td>Redistributing: eigrp 100</td>
</tr>
<tr>
<td>EIGRP NSF-aware route hold timer is 240s</td>
</tr>
<tr>
<td>Automatic network summarization is in effect</td>
</tr>
<tr>
<td>Automatic address summarization:</td>
</tr>
</tbody>
</table>
### EIGRP Features and Function

EIGRP is a Cisco proprietary routing protocol that combines the advantages of link-state and distance vector routing protocols. EIGRP may act like a link-state routing protocol as it uses a Hello protocol to discover neighbors and form neighbor relationships, and only partial updates are sent when a change occurs. However, EIGRP is still based on the key

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Mask</th>
<th>Summarizing with metric</th>
<th>Maximum path:</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.0/24</td>
<td>for Loopback0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>172.16.0.0/16</td>
<td>for Loopback100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Routing for Networks:**
- 172.16.1.0/24
- 192.168.1.0

**Routing Information Sources:**
- **Gateway** | **Distance** | **Last Update**
  - (this router) | 90 | 00:00:19

**Distance:** internal 90 external 170

Routing Protocol is "ospf 100"
- Outgoing update filter list for all interfaces is not set
- Incoming update filter list for all interfaces is not set
- Router ID 172.16.1.100
- Number of areas in this router is 1. 1 normal 0 stub 0 nssa
- Maximum path: 4

**Routing for Networks:**
- 255.255.255.255 0.0.0.0 area 0

**Reference bandwidth unit is 100 mbps**

**Routing Information Sources:**
- **Gateway** | **Distance** | **Last Update**
  - (default is 110)

Routing Protocol is "bgp 100"
- Outgoing update filter list for all interfaces is not set
- Incoming update filter list for all interfaces is not set
- IGP synchronization is disabled
- Automatic route summarization is disabled
- Maximum path: 1

**Routing Information Sources:**
- **Gateway** | **Distance** | **Last Update**
  - external 20 internal 200 local 200
distance vector routing protocol principle in which information about the rest of the network is learned from directly connected neighbors. EIGRP is an advanced distance vector routing protocol that includes the following features:

- **Rapid convergence:** EIGRP uses the DUAL algorithm to achieve rapid convergence. As the computational engine that runs EIGRP, DUAL is the main computational engine of the routing protocol, guaranteeing loop-free paths and backup paths (called *feasible successors*) throughout the routing domain. A router that uses EIGRP stores all available backup routes for destinations so that it can quickly adapt to alternate routes. If the primary route in the routing table fails, the best backup route is immediately added to the routing table. If no appropriate route or backup route exists in the local routing table, EIGRP queries its neighbors to discover an alternate route.

- **Load balancing:** EIGRP supports both equal and unequal metric load balancing, which allows administrators to better distribute traffic flow in their networks.

- **Loop-free, 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 subnets and variable-length subnet masks (VLSM).

- **Reduced bandwidth usage:** EIGRP uses the terms *partial* and *bounded* when referring to its updates. EIGRP does not make periodic updates. *Partial* means that the update includes only information about the route changes. EIGRP sends these incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table. *Bounded* refers to the propagation of partial updates that are sent specifically to those routers that are affected by the changes. By sending only the necessary routing information to those routers that need it, EIGRP minimizes the bandwidth required to send EIGRP updates. EIGRP uses multicast and unicast rather than broadcast. Multicast EIGRP packets employ the reserved multicast address of 224.0.0.10. As a result, end stations are unaffected by routing updates and requests for topology information.

EIGRP has four basic components:

- Neighbor discovery/recovery
- Reliable Transport Protocol
- DUAL finite state machine
- Protocol-dependent modules

Neighbor discovery/recovery is the process that routers use to dynamically learn about other routers on their directly attached networks. Routers must also discover when their neighbors become unreachable or inoperative. This process is achieved with low overhead by periodically sending small hello packets. As long as hello packets are received, a router can determine that a neighbor is alive and functioning. Once this is confirmed, the neighboring routers can exchange routing information.
The reliable transport protocol (not to be confused with Real Time Protocol-RTP, which is used to carry Voice over IP traffic) is responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors. It supports the simultaneous usage of multicast or unicast packets. Only some EIGRP packets must be transmitted perfectly. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities, such as Ethernet, sending hellos reliably to all neighbors individually is not required. So, EIGRP sends a single multicast hello with an indication in the packet informing the receivers that the packet does not need to be acknowledged. Other types of packets, such as updates, require acknowledgment, and that is indicated in the packet. The reliable transport protocol has a provision to send multicast packets quickly when there are unacknowledged packets pending. This ensures that convergence time remains low in the presence of links with varying speed.

The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. The distance information, known as a metric, is used by DUAL 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 where a new successor is determined. The amount of time it takes to recalculate the route affects the convergence time. Even though the recomputation is not processor-intensive, it is better to avoid it if possible. When a topology change occurs, DUAL tests for feasible successors. If there are feasible successors, it uses any it finds in order to avert any unnecessary recomputation. Feasible successors are defined in detail later in this book.

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

**EIGRP Packet Types**

EIGRP uses five packet types:

- Hello/ACKs
- Updates
- Queries
- Replies
- Requests
As stated earlier, hellos are multicast for neighbor discovery/recovery. They do not require acknowledgment. A hello with no data is also used as an acknowledgment (ACK). ACKs are always sent using a unicast address and contain a non-zero acknowledgment number.

Updates are used to give information on routes. When a new neighbor is discovered, update packets are sent so that the neighbor can build up its EIGRP topology table. In this case, update packets are unicast. In other cases, such as a link cost change, updates are multicast.

Queries and replies are used for finding and conveying routes. Queries are always multicast unless they are sent in response to a received query. ACKs to queries always unicast back to the successor that originated the query. Replies are always sent in response to queries to indicate to the originator that it does not need to go into Active state because it has feasible successors. Replies are unicast to the originator of the query. Both queries and replies are transmitted reliably.

**Note** EIGRP has two other type of packets, but they are insignificant: request packets and IPX SAP packets. Request packets are specialized packets that were never fully implemented in EIGRP. EIGRP for Internet Packet Exchange (IPX) has IPX SAP packets. These packets have an optional code in them, technically making them another packet type.

**EIGRP Path Selection**

Each EIGRP router maintains a neighbor table. This table includes a list of directly connected EIGRP routers that have an adjacency with this router. Neighbor relationships are used to track the status of these neighbors. EIGRP uses a low-overhead Hello protocol to establish and monitor the connection status with its neighbors.

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 from its directly connected EIGRP neighbors. EIGRP chooses the best routes to a destination from the topology table and places these routes in the routing table.

Figure 3-4 gives an example of the neighbor table, the topology table, and the subsequent derived routing table from the example.
To determine the best route (successor) and any backup routes (feasible successors) to a destination, EIGRP uses the following two parameters:

- **Advertised distance (AD):** The EIGRP metric for an EIGRP neighbor to reach a particular network.

- **Feasible distance (FD):** The AD for a particular network that is learned from an EIGRP neighbor plus the EIGRP metric to reach that neighbor. This sum provides an end-to-end metric from the router to that remote network. A router compares all FDs to reach a specific network and then selects the lowest FD and places it in the routing table.

The EIGRP topology table contains all of the routes that are known to each EIGRP neighbor. As shown in Figure 3-4, Routers A and B sent their routing tables to Router C, whose table is displayed. Both Routers A and B have routes to network 10.1.1.0/24 as well as to other networks that are not shown.

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 metric (1000) to the respective AD for each route, and the results represent the FDs that Router C must travel to reach network 10.1.1.0/24.

Router C chooses the least FD (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 FD that is installed in the routing table is called the **successor route**.

If one or more feasible successor routes exist, Router C chooses a backup route to the successor, called a **feasible successor route**. To become a feasible successor, a route must
satisfy this feasibility condition: a next-hop router must have an AD that is less than the FD of the current successor route. (Hence, the route is tagged as a feasible successor, which is a loop-free path to the destination). This rule is used to ensure that the network is loop-free.

If the route via 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. A route changes from a passive state to an active state (actively sending queries to neighboring routers for alternative routes) if a feasible successor does not exist and recomputation is necessary to determine the new successor.

Note  In Figure 3-4, values for the EIGRP metric and for FDs and ADs are simplified to make the scenario easier to understand. The metrics in a real-world example would normally be larger.

Understanding the EIGRP Metric

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

- **Bandwidth**: The smallest bandwidth of all outgoing interfaces between the source and destination in kilobits per second.
- **Delay**: The cumulative (sum) of all interface delay along the route in tenths of microseconds.

The following criteria also can be used for the EIGRP metric, but using them is 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, which is based on keepalives.
- **Load**: This value represents the worst load on a link between the source and destination, which is computed based on the packet rate and the configured bandwidth of the interface.
- **K values**: K values are administratively set parameters that manipulate the value of the EIGRP Metrics. Changing them is not recommended. They are involved in the metric calculation and are set to 1 and 0 to default. This way, the default K values do not affect the metric (K1, K3 are one – K1, K4, K5 are zero). The K values are
  - K1 = Bandwidth modifier
  - K2 = Load modifier
  - K3 = Delay modifier
K4 = Reliability modifier

K5 = Additional Reliability modifier

The composite metric formula is used by EIGRP to calculate metric value. The formula consists of values K1 through K5, which are known as EIGRP metric weights. By default, K1 and K3 are set to 1, and K2, K4, and K5 are set to 0. The result is that only the bandwidth and delay values are used in the computation of the default composite metric. The metric calculation method (K values) and the EIGRP AS number must match between EIGRP neighbors. Figure 3-5 shows a sample metric calculation with default K values and scaled metrics.

EIGRP uses scaled values to determine the total metric: 256 * ([K1 * bandwidth] + [K2 * bandwidth] / [256 – Load] + K3 * Delay) * (K5 / [Reliability + K4]), where if K5 = 0, the (K5 / [Reliability + K4]) part is not used (that is, equals to 1). Using the default K values, the metric calculation simplifies to 256 * (bandwidth + delay). Figure 3-5 gives the metrics in scaled values. Delay and bandwidth are scaled to mathematically fit the equation. 10^7 is used for bandwidth, and 10 is used for delay. This helps keep the metric as a manageable number.

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

![Figure 3-5 EIGRP Metric](image)

By using the `show interface` command, you can examine the actual values that are used for bandwidth, delay, reliability, and load in the computation of the routing metric. The output in Example 3-2 shows the values that are used in the composite metric for the Serial0/0/0 interface.

**Example 3-2 show interface to Verify the EIGRP Metric**

```
HQ# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is down
   Hardware is GT96K Serial   Description: Link to Branch
   MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
       reliability 255/255, txload 1/255, rxload 1/255
<output truncated>
```
**EIGRP Basic Configuration**

The `router eigrp` global configuration command enables EIGRP. Use the `router eigrp` and `network` commands to create an EIGRP routing process. Note that EIGRP requires an AS number. The AS parameter is a number between 1 and 65,535 that is chosen by the network administrator and must match all routers in the EIGRP AS. The `network` command is used in the router configuration mode.

Figure 3-6 shows a sample two-node network that is the basis for the following examples explaining how to configure EIGRP.

![Figure 3-6 Example Network for EIGRP Configuration](image)

Example 3-6 shows a sample two-node network that is the basis for the following examples explaining how to configure EIGRP.

**Example 3-3 Configuring EIGRP on the Branch Router**

```
Branch(config)# router eigrp 100
Branch(config-router)# network 10.1.1.0
Branch(config-router)# network 192.168.1.0
```

Example 3-4 shows how to configure EIGRP on the HQ router.

**Example 3-4 Configuring EIGRP on the HQ Router**

```
HQ(config)# router eigrp 100
HQ(config-router)# network 172.16.1.0 0.0.0.255
HQ(config-router)# network 192.168.1.0 0.0.0.255
```

Table 3-2 describes the EIGRP commands in detail.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>router eigrp as_number</code></td>
<td>Enables the EIGRP routing process for the AS number that is specified.</td>
</tr>
<tr>
<td><code>network network_id wildcard_mask</code></td>
<td>Associates the network with the EIGRP routing process. Use of the wildcard mask to match multiple networks is optional.</td>
</tr>
</tbody>
</table>
In Examples 3-3 and 3-4 the `router eigrp` and `network` commands were used to create an EIGRP routing process. Note that EIGRP requires an AS number. In this case, the AS number is 100 on both routers, because the AS parameter must match in all EIGRP routers for the formation of neighbor adjacency and for routes to be exchanged.

The `network` command defines a major network number to which the router is directly connected. Any interface on this router that matches the network address in the `network` command is enabled to send and receive EIGRP updates. The EIGRP routing process searches for interfaces that have an IP address that belongs to the networks specified with the `network` command. The EIGRP process begins on these interfaces. As you can see in Example 3-5, the EIGRP process is running on the interface. However, a second EIGRP process has been configured, but it does not match any interfaces in the `network` command.

### Example 3-5  Reviewing the EIGRP Neighbors

<table>
<thead>
<tr>
<th>HQ# show ip eigrp neighbors</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-EIGRP neighbors for process 100</td>
</tr>
<tr>
<td>H</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>


### Verification of EIGRP Configuration and Operation

Use the `show ip eigrp neighbors` command to display the neighbors that EIGRP discovered and determine when they become active and inactive. The command is also useful for debugging when neighbors are not communicating properly.

As you can see in Figure 3-7, the Branch router has a neighbor relationship with the HQ router, which is also shown in the following command output:

<table>
<thead>
<tr>
<th>Branch# show ip eigrp neighbors</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-EIGRP neighbors for AS(100)</td>
</tr>
<tr>
<td>H</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>
Verify EIGRP Neighbors

10.1.1.0/24 Branch S0/0/0 192.168.1.1 192.168.1.2
HQ S0/0/0 172.16.1.10/24

Figure 3-7  Verification of EIGRP Configuration with *show ip eigrp neighbors* Command

Table 3-3 identifies the key fields in the output of *show ip eigrp neighbors* command.

**Table 3-3**  *Key Output Fields from show ip eigrp neighbors Command*

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>AS identifier for this EIGRP process.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface that EIGRP receives hello packets from the neighbor on.</td>
</tr>
<tr>
<td>Hold</td>
<td>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.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Elapsed time (in hours:minutes:seconds) since the local router first heard from this neighbor.</td>
</tr>
<tr>
<td>Q Cnt</td>
<td>Number of EIGRP packets (update, query, and reply) that the software is waiting to send.</td>
</tr>
<tr>
<td>Seq Num</td>
<td>Sequence number of the last update, query, or reply packet that was received from this neighbor.</td>
</tr>
</tbody>
</table>

Use the *show ip eigrp interfaces* command to determine active EIGRP interfaces and learn information regarding those interfaces. If you specify an interface (for example, *show ip eigrp interfaces FastEthernet0/0*), only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are shown. If you specify an AS (for example, *show ip eigrp interfaces 100*), the only thing displayed is the routing process for the specified AS. Otherwise, all EIGRP processes are shown.

Table 3-4 defines the fields in *show ip eigrp interfaces*. 
### Table 3-4  Key Output Fields from `show ip eigrp interfaces` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface that EIGRP is configured on.</td>
</tr>
<tr>
<td>Peers</td>
<td>List of directly connected EIGRP neighbors.</td>
</tr>
<tr>
<td>Xmit Queue Unreliable/Reliable</td>
<td>Number of packets remaining in the Unreliable and Reliable queues.</td>
</tr>
<tr>
<td>Mean SRTT</td>
<td>Mean smooth round-trip time (SRTT) interval (in milliseconds).</td>
</tr>
<tr>
<td>Pacing Time Un/Reliable</td>
<td>Pacing time (how long to wait) used to determine when EIGRP packets should be sent out the interface (Unreliable and Reliable packets).</td>
</tr>
<tr>
<td>Multicast Flow Timer</td>
<td>Maximum number of seconds that the router will wait for an ACK packet after sending a multicast EIGRP packet, before switching from multicast to unicast.</td>
</tr>
<tr>
<td>Pending Routes</td>
<td>Number of routes in the packets sitting in the transmit queue waiting to be sent.</td>
</tr>
</tbody>
</table>

The `show ip route` command, as seen in the next section, in Example 3-6, displays the current entries in the routing table. EIGRP has a default administrative distance of 90 for internal routes and 170 for routes that are redistributed (redistributed routes are routes brought into a routing protocol from an external source; a routing protocol or static routes). When compared to other IGPs, EIGRP is the most preferred by Cisco IOS Software because it has the lowest administrative distance.

### EIGRP Passive Interfaces

Most routing protocols have a passive interface. A passive interface suppresses some routing updates but also allows other updates to be exchanged normally. EIGRP is slightly different from other routing protocols. Routing updates are not received and processed. No neighbor relationships are established via a passive interface.

Passive interfaces are set in EIGRP configuration mode, as shown next, and are not configured on the interface:

```plaintext
router eigrp 1
passive-interface FastEthernet0/0
```

This sets passive interface status on FastEthernet0/0. The following sets passive interface status as the default behavior, and explicitly specifies which interfaces should not be “passive”:

```plaintext
router eigrp 1
passive-interface default
no passive-interface FastEthernet0/0
```
This sets all interfaces to passive, except FastEthernet0/0.

Figure 3-8 displays a sample network for verification using the `show ip route` command.

![Figure 3-8: Verification of EIGRP Configuration with show ip route Command](image)

The routing table is shown in Example 3-6.

**Example 3-6  Reviewing the Routing Table Using Passive Interfaces**

<table>
<thead>
<tr>
<th>Branch#</th>
<th><code>show ip route</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes:</td>
<td>C - connected, S - static, R - RIP, M - mobile, B - BGP</td>
</tr>
<tr>
<td></td>
<td>D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area</td>
</tr>
<tr>
<td></td>
<td>N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2</td>
</tr>
<tr>
<td></td>
<td>E1 - OSPF external type 1, E2 - OSPF external type 2</td>
</tr>
<tr>
<td></td>
<td>i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2</td>
</tr>
<tr>
<td></td>
<td>ia - IS-IS inter area, * - candidate default, U - per-user static route</td>
</tr>
<tr>
<td></td>
<td>o - ODR, P - periodic downloaded static route</td>
</tr>
</tbody>
</table>

Gateway of last resort is not set

```
10.0.0.0/24 is subnetted, 1 subnets
C   10.1.1.0/24 is directly connected, GigabitEthernet0/0
L   10.1.1.1/32 is directly connected, GigabitEthernet0/0
172.16.0.0/24 is subnetted, 1 subnets
D   172.16.1.0 [90/156160] via 192.168.1.2, 02:02:02, Serial 0/0/0
192.168.1.0/24 is subnetted, 1 subnets
C   192.168.1.0/24 is directly connected, Serial0/0/0
L   192.168.1.1/32 is directly connected, Serial0/0/0
```

For the example network depicted in Example 3-7, the `show ip eigrp topology` command displays the EIGRP topology table, the active or passive state of routes, the number of successors, and the FD to the destination. Use the `show ip eigrp topology all-links` command to display all paths, even those that are not feasible.
Figure 3-9  Verification of EIGRP Configuration with show ip eigrp topology Command

Example 3-7  Using the show ip eigrp topology Command

```
Branch# show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(192.168.1.1)

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

P 192.168.1.0/24, 1 successors, FD is 28160
   via Connected, Serial0/0/0
P 172.16.1.0/24, 1 successors, FD is 156160
   via 192.168.1.2 (156160/128256), Serial0/0/0
P 10.1.1.0/24, 1 successors, FD is 28160
   via Connected, GigabitEthernet0/0/0
```

Table 3-5 defines the fields in the show ip eigrp topology command.

Table 3-5  Key Output Fields from show ip eigrp topology Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>P – Passive: No EIGRP computations are being performed for this destination.</td>
<td></td>
</tr>
<tr>
<td>A – Active: EIGRP computations are being performed for this destination.</td>
<td></td>
</tr>
<tr>
<td>U – Update: An update packet was sent to this destination.</td>
<td></td>
</tr>
<tr>
<td>Q – Query: A query packet was sent to this destination.</td>
<td></td>
</tr>
<tr>
<td>R – Reply: A reply packet was sent to this destination.</td>
<td></td>
</tr>
<tr>
<td>r – Reply status Flag that is set after the software has sent a query and is waiting for a reply.</td>
<td></td>
</tr>
</tbody>
</table>
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.0 /24</td>
<td>Destination IP network number and bits in the subnet mask (/24=255.255.255.0)</td>
</tr>
<tr>
<td>successors</td>
<td>Number of successors. This number corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or next hop is in a transition state.</td>
</tr>
<tr>
<td>FD</td>
<td>Feasible distance. The FD 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 advertised distance (AD) of the router (the metric after the slash) is less than the FD, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it does not need to send a query for that destination.</td>
</tr>
<tr>
<td>replies</td>
<td>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.</td>
</tr>
<tr>
<td>via</td>
<td>IP address of the peer that informed 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.</td>
</tr>
<tr>
<td>(156160/128256)</td>
<td>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.</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>Interface from which this information was learned.</td>
</tr>
</tbody>
</table>

### Load Balancing with EIGRP

Every routing protocol supports equal-cost path load balancing, which is the ability of a router to distribute traffic over all of 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. EIGRP also supports unequal-cost path load balancing. You use the `variance n` command to instruct the router to include routes with a metric of less than n times the minimum metric route for that destination. The variable n can take a value between 1 and 128. The default is 1, which specifies equal-cost load balancing. Traffic is also distributed among the links with unequal costs, proportionately, with respect to the metric.
Here’s a quick comparison of the two types of load balancing offered by EIGRP:

- **Equal-cost load balancing**
  - By default, up to four routes with a metric equal to the minimum metric are installed in the routing table.
  - By default, the routing table can have up to 16 entries for the same destination.

- **Unequal-cost load balancing**
  - By default, it is not turned on.
  - Load balancing can be performed through paths that are 128 times less desirable than the route with the lowest FD.

For IP, Cisco IOS Software applies load balancing across up to four equal-cost paths by default. With the `maximum-paths` router configuration command, up to 32 equal-cost routes can be kept in the routing table, depending on the router type and Cisco IOS version. If you set the value 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.

Per-packet load balancing is problematic for applications such as voice and video, which require packets to arrive in order. Per-destination switching is the default and must be changed to per-packet using the interface command `ip load-sharing per-packet`. Unless your network is free of applications that require packets in order, changing this parameter is not recommended.

**Variance**

This section provides an example of variance for the sample network depicted in Figure 3-10.

![Figure 3-10 Example Network to Display Metrics](image-url)
In Figure 3-10, there are three ways to get from Router E to Network X:

- E-B-A with a metric of 30
- E-C-A with a metric of 20
- E-D-A with a metric of 45

Router E chooses the path E-C-A with a metric of 20 because 20 is better than 30 and 45. To instruct EIGRP to select the path E-B-A as well, you would configure `variance` with a multiplier of 2:

```
router eigrp 1
network x.x.x.x variance 2
```

This configuration increases the minimum metric to 40 (2 * 20 = 40). EIGRP includes all routes that have a metric of less than or equal to 40 and satisfy the feasibility condition. The configuration in this section illustrates that EIGRP now uses two paths to reach Network X, E-C-A and E-B-A, because both paths have a metric of under 40. EIGRP does not use path E-D-A because that path has a metric of 45, which is not less than the value of the minimum metric of 40 because of the variance configuration. Also, the AD of neighbor D is 25, which is greater than the FD of 20 through C. This means that, even if variance is set to 3, the E-D-A path is not selected for load balancing because Router D is not a feasible successor.

**Traffic Sharing**

EIGRP provides not only unequal-cost path load balancing, but also intelligent load balancing, such as traffic sharing. To control how traffic is distributed among routes when multiple routes for the same destination network have different costs, use the `traffic-share balanced` command. With the keyword `balanced`, the router distributes traffic proportionately to the ratios of the metrics that are associated with different routes. This is the default setting:

```
router eigrp 1
network x.x.x.x variance 2
traffic-share balanced
```

The traffic share count for the example in Figure 3-10 is

- For path E-C-A: $30 / 20 = 3 / 2 = 1$
- For path E-B-A: $30 / 30 = 1$

Because the ratio is not an integer, you round down to the nearest integer. In this example, EIGRP sends one packet to E-C-A and one packet to E-B-A.

If we change the metric between links E and B in the example, the result would be the change in metric between B and A changes to 15. In this case, the E-B-A metric is 40. However, this path will not be selected for load balancing because the cost of this path,
40, is not less than \((20 \times 2)\), where 20 is the FD and 2 is the variance. To also include this path in load sharing, the variance should be changed to 3. In this case, the traffic share count ratio is

- For path E-C-A: \(\frac{40}{20} = 2\)
- For path E-B-A: \(\frac{40}{40} = 1\)

In this situation, EIGRP sends two packets to E-C-A and one packet to E-B-A. Therefore, EIGRP provides both unequal-cost path load balancing and intelligent load balancing.

Similarly, when you use the `traffic-share` command with the keyword `min`, the traffic is sent only across the minimum-cost path, even when there are multiple paths in the routing table:

```cisco
router eigrp 1
network x.x.x.x variance 3
    traffic-share min across-interfaces
```

In this situation, EIGRP sends packets only through E-C-A, which is the best path to the destination network. This is identical to the forwarding behavior without use of the `variance` command. However, if you use the `traffic-share min` command and the `variance` command, even though traffic is sent over the minimum-cost path only, all feasible routes get installed into the routing table, which decreases convergence times.

### EIGRP Authentication

Many routing protocols allow the addition of some sort of authentication to protect against accepting routing messages from other routers that are not configured with the same preshared key. If this authentication is not configured, a malicious or misconfigured device can be introduced into the network. This may inject different or conflicting route information into the network, causing loss of service.

To configure EIGRP authentication, the router must first be configured globally with a “key chain,” using the `key chain` command in global configuration mode. Then, each interface that uses EIGRP must be configured individually in the device. In Example 3-9, MD5 type key encryption is used.

**Example 3-8 Configuring EIGRP Authentication**

```bash
Branch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)# key chain 1
Branch(config-keychain)# exit
Branch(config)# key chain key4eigrp
Branch(config-keychain)# key 1
Branch(config-keychain-key)# key-string secureeigrp
Branch(config-keychain-key)# exit
```
With the global key chain configured, other applications, besides EIGRP, such as the RIP version 2 routing protocol, can now use this key chain. Next, apply it to the EIGRP interface configuration. EIGRP authentication is on a per-link basis. Neighboring interfaces must be configured with the same key chain. Other interfaces can be configured with other key chains or can have no authentication, as long as all neighbors are configured similarly. Example 3-9 provides the configuration necessary for application of the key chain to a single interface. The routers that are directly connected neighbors from interface FastEthernet0/0 in Example 3-9 must use the same authentication mode and the same key chain.

Example 3-9  

**Placing Authentication on an Interface**

```plaintext
Branch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)# interface FastEthernet0/0
Branch(config-if)# ip authentication mode eigrp 100 md5
Branch(config-if)# ip authentication key-chain eigrp 100 key4eigrp
Branch(config-if)# exit
```

**Note**  For more information on EIGRP authentication, see the Cisco document “EIGRP Message Authentication Configuration Example” at http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a00807f5a63.shtml.

**Troubleshooting EIGRP**

The ability to troubleshoot problems related to the exchange of routing information and missing information from the routing table is one of the most essential skills for a network engineer who is involved in the implementation and maintenance of a routed enterprise network that uses a routing protocol.

This section provides a suggested troubleshooting flow and explains the Cisco IOS commands that you can use to gather information from the EIGRP data structures and routing processes to detect and correct routing issues.

**Components of Troubleshooting EIGRP**

In troubleshooting EIGRP, as with any networking issue, follow a structured methodology. Figure 3-11 shows a suggested flowchart.
Connectivity issues

Does the neighbors table hold all the devices that you expect?

- Are interfaces operational?
- Does the EIGRP AS match?
- Are the interfaces enabled for EIGRP?
- Is there an interface that is configured as passive?

Yes
- Does the routing table have all the necessary routes?
- Are the networks being advertised?
- Is there an ACL blocking advertisements?
- Is there a discontiguous network issue?

Yes
- Functional network

No

Figure 3-11 EIGRP Troubleshooting Flowchart

After configuring EIGRP, first test connectivity to the remote network, using ping. If the ping fails, check that the router has EIGRP neighbors and troubleshoot on a link-by-link basis. Neighbor adjacency might not be running for a number of reasons. Figure 3-12 provides a very basic design with two EIGRP neighbors connected by an Ethernet switch. The HQ router has three loopback interfaces, and both routers have two FastEthernet interfaces. One FastEthernet (0/0) interface from each router is connected to a switch. The switch has only one VLAN for all ports.

Figure 3-12 Simple Network Example

Now let’s examine a few potential scenarios, via `show` commands:

- The interface between the devices is down:

  HQ# show ip interface brief
<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>192.168.1.20</td>
<td>YES</td>
<td>NVRAM</td>
<td>down</td>
<td>down</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>10.5.0.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Loopback1</td>
<td>5.5.5.5</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Loopback30</td>
<td>2.2.2.2</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Loopback100</td>
<td>1.1.1.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
In this case, FastEthernet0/0 is down. Possibilities include a disconnected cable, a down switch, or faulty hardware.

- The two routers have mismatching EIGRP AS numbers:

  ```
  HQ# show ip protocol
  Routing Protocol is "eigrp 1"
  <output omitted>
  
  Branch# show ip protocol
  Routing Protocol is "eigrp 10"
  <output omitted>
  ```

  In this case, the Branch and HQ routers are misconfigured with different EIGRP AS numbers.

- Proper interfaces are not enabled for the EIGRP process:

  ```
  HQ# show running-config
  <output omitted>
  router eigrp 1
  network 192.168.1.0 255.255.255.0
  <output omitted>
  
  HQ# show ip interface brief
  Interface          IP-Address         OK?    Method     Status        Protocol
  FastEthernet0/0    192.168.1.20       YES    NVRAM      up            up
  FastEthernet0/1    10.5.0.1           YES    NVRAM      up            up
  Loopback1          5.5.5.5            YES    NVRAM      up            up
  Loopback30         2.2.2.2            YES    NVRAM      up            up
  Loopback100        1.1.1.1            YES    NVRAM      up            up
  
  In this case, there is only a single interface configured for EIGRP.

- The interface between the devices is up but can’t ping:

  ```
  HQ# show ip interface brief
  Interface          IP-Address         OK?    Method     Status        Protocol
  FastEthernet0/0    192.168.1.20       YES    NVRAM      up            up
  FastEthernet0/1    10.5.0.1           YES    NVRAM      up            up
  Loopback1          5.5.5.5            YES    NVRAM      up            up
  Loopback30         2.2.2.2            YES    NVRAM      up            up
  Loopback100        1.1.1.1            YES    NVRAM      up            up
  Branch# show ip interface brief
  Interface          IP-Address         OK?    Method     Status        Protocol
  FastEthernet0/0    192.168.1.25       YES    NVRAM      up            up
  FastEthernet0/1    10.20.0.1          YES    NVRAM      up            up
  
  In this case, a potential Layer 2 problem exists. This could be a misconfigured switch port and/or VLAN misconfiguration.
An interface is configured as passive:

HQ# show running-config
<output omitted>
router eigrp 1
  passive-interface FastEthernet0/0
network 192.168.1.0 255.255.255.0
<output omitted>

In this case, a passive-interface is configured. The show ip protocols command will also identify passive interfaces.

Aside from the issues reviewed here, there are a number of other, more advanced concerns that can prevent neighbor relationships from forming. Two examples are misconfigured EIGRP authentication or mismatched K values, depending on which EIGRP calculates its metric. The next section covers specifically neighbor adjacency.

Troubleshooting EIGRP Neighbor Issues

The previous section examined several possible reasons why EIGRP might not be working properly. This section takes a closer look at troubleshooting EIGRP neighbor relationships. As previously mentioned, a major prerequisite for the neighbor relationship to form between routers is Layer 3 connectivity. By investigating the output of show ip interface brief, you can verify that the status and protocol are both up for the interface between the routers. In Figure 3-13 and Example 3-10, the Serial0/0/0 interface that is connected to the Branch router is up. A successful ping then confirms IP connectivity between routers.

![Figure 3-13 Determining If the Interface Is Operational](image)

**Example 3-10 Verifying Protocol and Status of Link Between Neighbors**

<table>
<thead>
<tr>
<th>Branch# show ip interface brief</th>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GigabitEthernet0/0</td>
<td>10.1.1.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td></td>
<td>Serial0/0/0</td>
<td>192.168.1.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Branch# ping 192.168.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type escape sequence to abort.
If the ping is not successful, as shown in Example 3-10, you should use the technologies discussed in Chapter 2, “Troubleshooting Basic Connectivity.” First, check the cabling and verify that the interfaces on connected devices are on a common subnet.

If you notice a log message such as the following that states that EIGRP neighbors are “not on common subnet,” this indicates that there is an improper IP address on one of the two EIGRP neighbor interfaces:

*Mar 28 04:04:53.778: IP-EIGRP(Default-IP-Routing-Table:100): Neighbor 192.168.100.1 not on common subnet for Serial0/0/0

If this message was received on the Branch router, you can see that the reported IP address of the neighbor does not match what you expected. However, you can still have an IP address mismatch and not see this message.

Next, check that the AS numbers are the same between neighbors. The command that starts the EIGRP process is followed by the AS number, `router eigrp as_number`. This AS number is significant to the entire network, as it must match between all the routers within the same routing domain. In other routing protocols, the numbering used to start the process may have only local significance (for instance, the OSPF routing protocol is started with a process-id and does not use an AS number).

In Figure 3-14 and Example 3-11, `show ip protocols` helps to determine if the AS numbers match.

![Figure 3-14 Determining AS Numbers](image)

**Example 3-11 Using show ip protocols to Verify EIGRP AS Numbers**

```bash
Branch# show ip protocols
Routing Protocol is “EIGRP 1”
<output omitted>

HQ# show ip protocols
Routing Protocol is “EIGRP 2”
<output omitted>
```
Also confirm that EIGRP is running on the correct interfaces. The **network** command configured under the EIGRP routing process indicates which router interfaces will participate in EIGRP.

The **show ip eigrp interfaces** command shows you which interfaces are enabled for EIGRP. If connected interfaces are not enabled for EIGRP, then neighbors will not form an adjacency. If an interface is not on the list, that means the router is not communicating EIGRP through that interface. Figure 3-15 shows that EIGRP is running on the Branch router. Run the same command on the HQ router and look for the same results. In this case, both routers are neighbors.

**Figure 3-15  EIGRP Interface Enabled**

You can also check the interface by referring to the “Routing for Networks” section of the **show ip protocols** command output. As shown in Example 3-12, this indicates which networks have been configured; any interfaces in those networks participate in EIGRP.

**Example 3-12  Check the “Routing for Networks” Output**

```plaintext
HQ# show ip protocols
<output omitted>
Routing Protocol is "eigrp 1"
<output omitted>
Routing for Networks:
  172.16.0.0
  192.168.1.0
Passive Interface(s):
  Serial0/0/0
<output omitted>
```

With the **show ip protocols** command, you can also confirm if an interface is in passive mode only. The **passive-interface** command prevents both outgoing and incoming routing updates, because the effect of the command causes the router to stop sending and receiv-
ing hello packets over an interface. For this reason, routers do not become neighbors. An example where you would need to configure an interface as passive toward a specific LAN. You want to advertise LANs but don't want to have the security risk of transmitting hello packets into the LAN. A final suggestion for checking a failed neighbor relationship is to confirm a mismatch in the authentication parameters. The key authentication configuration must match on both neighbors. The key number and key string should be checked in the running configuration.

**Troubleshooting EIGRP Routing Table Issues**

This section covers issues that cause missing entries in the routing table when proper connectivity and neighbor relationships exist. The exclusion of routes that should be in the routing table can be caused by routes not being advertised, by route filtering, or by network summarization. Missing routing entries due to these issues can be related to a problem either with a directly connected EIGRP neighbor or with an EIGRP router that is in another section of the network.

**Issues Caused by Unadvertised Routes**

Routing table issues caused by unadvertised routes are indicated by a failed ping test. Figure 3-16 illustrates the Branch/HQ example that has been implemented. It is established by checking the neighbor adjacency.

![Figure 3-16](image)

**Figure 3-16**  *Troubleshooting EIGRP Routing Table Issues with the show ip protocols Command*

In this case, checking the `show ip protocols` command output from the HQ router indicates the HQ router is not advertising 172.16.1.0/24. Adding the `network` statement to EIGRP, as demonstrated in Example 3-13, should resolve the issue.

**Example 3-13**  *Adding the Correct Network Command*

```
HQ(config)# router eigrp 1
HQ(config-router)# network 172.16.1.0
```

This should restore the routing table. If it does not, check route filtering. Route filtering can be performed by route maps or ACLs, as discussed in the next section.
Issues Caused by Route Filtering

Routing protocols can be configured to filter routes. This is a powerful tool, especially when connecting different routing domains (different AS). However, a misconfigured filter can be difficult to detect.


When investigating filtering issues, first check the show ip protocols command, as demonstrated in Example 3-14.

Example 3-14 Identifying Incoming Filtering

<table>
<thead>
<tr>
<th>Branch#</th>
<th>show ip protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routing Protocol is “eigrp 1”</td>
</tr>
<tr>
<td></td>
<td>Outgoing update filter list for all interfaces is not set</td>
</tr>
<tr>
<td></td>
<td>Incoming update filter list for all interfaces is 1</td>
</tr>
</tbody>
</table>

As you can see, there is an ACL. Next, check the ACL, as shown in Example 3-15.

Example 3-15 Identifying Access List Used for Filtering

<table>
<thead>
<tr>
<th>Branch#</th>
<th>show ip access-lists</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standard IP access list 1</td>
</tr>
<tr>
<td></td>
<td>10 deny 172.16.0.0, wildcard bits 0.0.255.255 (2 matches)</td>
</tr>
<tr>
<td></td>
<td>20 permit any (6 matches)</td>
</tr>
</tbody>
</table>

The ACL matches the missing network. In this case, remove the ACL from the EIGRP configuration, as demonstrated in Example 3-16.

Example 3-16 Removing the Distribute List Used for Filtering

<table>
<thead>
<tr>
<th>Branch#</th>
<th>config t</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td>Branch(config)# router eigrp 1</td>
</tr>
<tr>
<td></td>
<td>Branch(config-router)# no distribute-list 1 in</td>
</tr>
</tbody>
</table>
The console output shows the change in the adjacency after changing the configuration, as demonstrated in Example 3-17.

**Example 3-17  Console Reporting Neighbor Change Due to Reconfiguration**

*Mar 1 00:17:37.775: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.1.1 (FastEthernet0/0) is down: route configuration changed

*Mar 1 00:17:41.431: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.1.1 (FastEthernet0/0) is up: new adjacency

**Caution**  Do not remove an actual ACL without first removing the ACL reference from other configuration/interfaces. Otherwise, you may create instability in the configuration!

Take notice of the “in” on the **distribute-list**. ACLs can be placed in both inbound and outbound directions. Inbound and outbound lists are structured the same, but the transmission or reception of routes is controlled by direction.

**Issues Caused by Automatic Network Summarization**

EIGRP can be configured to automatically summarize routes at classful boundaries. If you have discontiguous networks, automatic summarization can cause inconsistencies in the routing tables.

In Figure 3-17, Router B is not receiving individual routes for the 172.16.1.0/24 and 172.16.2.0/24 subnets. Both Router A and Router C automatically summarized those subnets to the 172.16.0.0/16 classful boundary when sending EIGRP update packets to Router C.

![Figure 3-17 Automatic Summarization Issues](image)

Router B has two routes to 172.16.0.0/16 in the routing table, which can result in inaccurate routing and packet loss, as shown in Example 3-18.
Example 3-18  *Inaccurate Routing Entries*

```
RouterB# show ip route
<output omitted>

Gateway of last resort is not set
10.0.0.0/24 is subnetted, 2 subnets
C  10.1.1.0 is directly connected, Serial0/2/0
C  10.2.2.0 is directly connected, Serial0/3/0
D  172.16.0.0/16 [90/2172416] via 10.1.1.1, 00:03:51, Serial0/2/0
    [90/2172416] via 10.2.2.3, 00:00:14, Serial0/3/0
```

**Note**  The behavior of the `auto-summary` command is disabled by default on Cisco IOS version 15. Older versions of Cisco IOS Software may have automatic summarization enabled by default.

In Example 3-19, automatic summarization is disabled by entering the `no auto-summary` command in the router eigrp configuration mode:

Example 3-19  *Disable Automatic Summarization*

```
RouterB(config)# router eigrp 1
RouterB(config-if)# no auto-summary
```

### Implementing EIGRP for IPv6

Although EIGRP is a Cisco proprietary protocol, it and its predecessor, IGRP (IGRP is an obsolete protocol and removed from production in Cisco IOS 12.3 and later), have been widely deployed in enterprise networks. EIGRP has also supported multiple protocols besides IP (AppleTalk and Novell IPX). For these reasons, it is logical that EIGRP would continue to be used in the IPv6 world. This section describes Cisco EIGRP support for IPv6. The theory and operation of EIGRP only differs slightly between IPv6 and IPv4. The main differences are where IPv6 and IPv4 deviate as a protocol, so parts of this section will serve as a review.

### EIGRP IPv6 Theory of Operation

Although the configuration and management of EIGRP for IPv4 and EIGRP for IPv6 are similar, they are configured and managed separately.

As previously mentioned, EIGRP is inherently a multiprotocol routing protocol because it has supported non-IP protocols. Novell IPX and AppleTalk were protocols with early support from EIGRP. As with the non-IP protocols, IPv6 support is added as a separate
module within the router. IPv6 EIGRP is configured and managed separately from IPv4 EIGRP, but the mechanisms and configuration techniques for IPv6 EIGRP will be very familiar to engineers who have worked with EIGRP for IPv4.

EIGRP maintains feature parity across protocols, where appropriate. Due to the differences in protocols, configuration and operation can slightly differ. Much of the theory in key areas such as DUAL and metrics are the same.

The following are a few (not all) examples of similarities shared by IPv4 EIGRP and IPv6 EIGRP:

- DUAL is used for route calculation and selection with the same metrics.
- It is scalable to large network implementations.
- Neighbor, routing, and topology tables are maintained.
- Both equal-cost load balancing and unequal-cost load balancing are offered.

A few (not all) examples of differences include these:

- The `network` command is not used in IPv6; EIGRP is configured via links.
- The `ipv6` keyword is used in many of the EIGRP commands.
- Needs to be explicitly enabled on each interface when configuring EIGRP.

The basic components of EIGRP for IPv6 remain the same as in the IPv4 version. So, this section contains a review of the operation of EIGRP and DUAL.

As in IPv4, EIGRP in IPv6 uses a hello packet to discover other EIGRP-capable routers on directly attached links and to form neighbor relationships. Updates may be acknowledged by using a reliable transport protocol, or they may be unacknowledged—depending on the specific function that is being communicated. The protocol provides the flexibility necessary to unicast or multicast updates, acknowledged or unacknowledged.

Hello packets and updates are set to the well-known, link-local multicast address FF02::A, which Cisco has obtained from the Internet Assigned Numbers Authority (IANA). This multicast distribution technique is more efficient than the broadcast mechanism that is used by earlier, more primitive routing protocols such as RIPv1. EIGRP for IPv4 also uses multicast for update distribution.

**Note** For more information on IANA numerical assignments, see http://www.iana.org/numbers.

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 that is required for EIGRP packets.
DUAL, which is an EIGRP algorithm for determining the best path through the network, uses several metrics to select efficient, loop-free paths. Figure 3-18 shows a topology with sample metrics. When multiple routes to a neighbor exist, DUAL determines which route has the lowest metric (the FD) and enters this route into the routing table. Other possible routes to this neighbor with larger metrics are received, and DUAL determines the AD to this network. The AD is defined as the total metric that is advertised by an upstream neighbor for a path to a destination. DUAL compares the AD with the FD, and if the AD is less than the FD, DUAL considers the route to be a feasible successor and enters the route into the topology table. The feasible successor route that is reported with the lowest metric becomes the successor route to the current route if the current route fails. To avoid routing loops, DUAL ensures that the AD is always less than the FD for a neighbor router to reach the destination network; otherwise, the route to the neighbor may loop back through the local router.

When there are no feasible successors to a route that has failed, but there are neighbors advertising the route, a recomputation must occur. This is the process where DUAL determines a new successor. The amount of time that is required to recompute the route affects the convergence time. Recomputation is processor-intensive, so avoiding unnecessary recomputation is advantageous. When a topology change occurs, DUAL tests for feasible successors. If there are feasible successors, DUAL uses them to avoid unnecessary recomputation of the topology.

![Figure 3-18](image-url)

**Figure 3-18  EIGRP Path Selection**

Of these metrics, by default, only minimum bandwidth and delay are used to compute the best path. Unlike most metrics, minimum bandwidth is set to the minimum bandwidth of the entire path, and it does not reflect how many hops or low-bandwidth links are in the path. Delay is a cumulative value that increases by the delay value of each segment in the path. In Figure 3-18, Router One is computing the best path to Network A.

It starts with the two advertisements for this network: one through Router Four, with a minimum bandwidth of 56 and a total delay of 2200; and the other through Router Three, with a minimum bandwidth of 128 and a delay of 1200. Router One chooses the path with the lowest metric.

Let’s compute the metrics. EIGRP calculates the total metric by scaling the bandwidth and delay metrics.
EIGRP uses the following formula to scale the bandwidth:

\[
\text{bandwidth} = \left(\frac{10000000}{\text{bandwidth}(i)}\right) \times 256
\]

where \( \text{bandwidth}(i) \) is the least bandwidth (represented in kilobits) of all outgoing interfaces on the route to the destination network.

EIGRP uses the following formula to scale the delay:

\[
\text{delay} = \text{delay}(i) \times 256
\]

where \( \text{delay}(i) \) is the sum of the delays configured on the interfaces, on the route to the destination network, in tens of microseconds. The delay as shown in the `show ipv6 eigrp topology` command or the `show interface` command is in microseconds, so you must divide by 10 before you use it in this formula. Throughout the section, a delay is used as it is configured and shown on the interface.

EIGRP uses these scaled values to determine the total metric to the network:

\[
\text{metric} = \left[ K1 \times \text{bandwidth} + \left( K2 \times \text{bandwidth} \right) / (256 - \text{load}) + K3 \times \text{delay} \right] \times \left[ K5 / (\text{reliability} + K4) \right]
\]

**Caution** You should not change these \( K \) values without first giving the decision careful consideration. Any revisions should be avoided and completed only after careful planning. Mismatched \( K \) values prevent a neighbor relationship from being built, which causes the network to fail to converge.

**Note** If \( K5 = 0 \), the formula reduces to \( \text{metric} = \left[ K1 \times \text{bandwidth} + \left( K2 \times \text{bandwidth} \right) / (256 - \text{load}) + K3 \times \text{delay} \right] \).

The default values for \( K \) are:

- \( K1 = 1 \)
- \( K2 = 0 \)
- \( K3 = 1 \)
- \( K4 = 0 \)
- \( K5 = 0 \)

For default behavior, you can simplify the formula as follows:

\[
\text{metric} = \text{bandwidth} + \text{delay}
\]

Cisco routers round down to the nearest integer to properly calculate the metrics. In this example, the total cost through Router Four is:

\[
\text{minimum bandwidth} = 56 \text{ kb total delay} = 100 + 100 + 2000 = 2200 \left(\frac{10000000}{56} + 2200\right) \times 256 = (178571 + 2200) \times 256 = 180771 \times 256 = 46277376
\]
And the total cost through Router Three is:

\[
\text{minimum bandwidth} = 128\text{kb} \quad \text{total delay} = 100 + 100 + 1000 = 1200 \\
\left(\frac{10000000}{128}\right) + 1200 \times 256 = 78125 + 1200 \times 256 = 79325 \times 256 = 20307200
\]

So to reach Network A, Router One chooses the route through Router Three.

Note that the bandwidth and delay values used are those configured on the interface through which the router reaches its next hop to the destination network. For example, Router Two advertised Network A with the delay configured on its Ethernet interface; Router Four added the delay configured on its Ethernet interface; and Router One added the delay configured on its serial interface.

When a router discovers a new neighbor, it records the neighbor address and interface as an entry in the neighbor table. One neighbor table exists for each protocol-dependent module (as stated earlier, EIGRP runs a protocol-independent module for each protocol running, so IPv4 and IPv6 are calculated independently). When a neighbor sends a hello packet, it advertises a hold time, which is the amount of time that a router treats a neighbor as reachable and operational. If a hello packet is not received within the hold time, the hold time expires and DUAL is informed of the topology change.

The topology table contains all destinations that are advertised by neighboring routers. Each entry in the topology table includes the destination address and a list of neighbors that have advertised the destination. For each neighbor, the entry records the advertised metric, which the neighbor stores in its routing table. An important rule that distance vector protocols must follow is that if the neighbor advertises this destination, the neighbor must use the route to forward packets. Although having a route and using it to forward packets may seem implicit, link-state protocols may advertise a route that is not necessarily a direct path. Explicitly, this can be done with the Border Gateway Protocol (BGP), but that topic is beyond the scope of this text.

**Note** As in IPv4, the MTU in IPv6 is carried in the EIGRP hello packets but is not used in the metric calculation.

**EIGRP IPv6 Feasible Successor**

As previously defined, the feasible distance is the best metric along a path to a destination network, including the metric to the neighbor advertising that path. Reported distance is the total metric along a path to a destination network as advertised by an upstream neighbor. A feasible successor is a path whose AD is less than the FD (current best path). Figure 3-19 illustrates this process.
Router One recognizes two routes to Network A, one through Router Three and another through Router Four:

- The route through Router Four has a cost of \(46277376\) and an AD of \(307200\).
- The route through Router Three has a cost of \(20307200\) and an AD of \(307200\).

Note that in each case, EIGRP calculates the AD from the router advertising the route to the network. In other words, the AD from Router Four is the metric to get to Network A from Router Four, and the AD from Router Three is the metric to get to Network A from Router Three. EIGRP chooses the route through Router Three as the best path, and uses the metric through Router Three as the FD. Because the AD to this network through Router Four is less than the FD, Router One considers the path through Router Four a feasible successor.

When the link between Routers One and Three goes down, Router One examines each path it knows to Network A and finds that it has a feasible successor through Router Four. Router One uses this route, using the metric through Router Four as the new FD. The network converges instantly, and updates to downstream neighbors are the only traffic from the routing protocol.

**EIGRP IPv6 Load Balancing**

Similarly to IPv4, IPv6 supports equal-cost load balancing and unequal-cost load balancing.

Cisco IOS Software has the ability to load balance across up to four equal-cost paths by default. With the `maximum-paths` router configuration command, up to 32 equal-cost routes can be kept in the routing table, depending on the router type and Cisco IOS version. If you set the value to 1, you disable equal-cost load balancing.

EIGRP supports unequal-cost path load balancing. Use the `variance n` command to instruct the router to include routes with a metric of less than \(n\) times the minimum metric route for that destination. The variable \(n\) can take a value between 1 and 128. The default is 1, which means equal-cost load balancing. Traffic is also distributed among the
links with unequal costs, proportionately, with respect to the metric. If a path is not a feasible successor, it is not used in load balancing.

**EIGRP for IPv6 Command Syntax**

This section covers some of the basics for EIGRP configuration under IPv6. Example 3-20 illustrates the process of basic IPv6 routing. It shows how to configure an IPv6 address and the EIGRP routing protocol on an interface, and verify that the EIGRP process has begun.

**Example 3-20  Configuring and Verifying EIGRP for IPv6**

```plaintext
IPv6-router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
IPv6-router(config)# interface FastEthernet0/0
IPv6-router(config-if)# ipv6 address 2001:DB8:A00:1::1/32
IPv6-router(config-if)# no shutdown
IPv6-router(config-if)# exit
IPv6-router(config)# ipv6 unicast-routing
IPv6-router(config)# ipv6 router eigrp 1
IPv6-router(config-rtr)# no shutdown
IPv6-router(config-rtr)# interface FastEthernet0/0
IPv6-router(config-if)# ipv6 eigrp 1
IPv6-router(config-if)# exit
IPv6-router(config)# exit
*Apr  8 06:56:18.011: %SYS-5-CONFIG_I: Configured from console by console
IPv6-router# show ipv6 protocol
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "eigrp 1"
   EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
   EIGRP maximum hopcount 100
   EIGRP maximum metric variance 1
Interfaces: FastEthernet0/0
Redistribution:       None
Maximum path: 16
Distance: internal 90 external 170
IPv6-router#
```

Table 3-6 describes the basic commands used in Example 3-20.
Table 3-6  Commands Used in Example 3-20

<table>
<thead>
<tr>
<th>Command(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface FastEthernet0/0</td>
<td>Enter interface mode</td>
</tr>
<tr>
<td>ipv6 address 2001:DB8:A00:1::1/32</td>
<td>Assign an IPv6 address on the interface</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>Enable IPv6 routing</td>
</tr>
<tr>
<td>ipv6 router eigrp 1</td>
<td>Configure EIGRP with AS number 1</td>
</tr>
<tr>
<td>no shutdown</td>
<td>Enable the EIGRP process</td>
</tr>
<tr>
<td>show ipv6 protocol</td>
<td>Verify the EIGRP process has started (more on EIGRP verification/show commands in the next section)</td>
</tr>
</tbody>
</table>


Verification of EIGRP IPv6 Operation

Example 3-21 shows the EIGRP topology for IPv6. A good point to note is that the command execution and information displayed are similar to the IPv4 version of the command (see Figure 3-7), and are just differentiated by the IPv4 and IPv6 protocol differences.

Example 3-21  EIGRP Topology for IPv6

```
IPv6-router# show ipv6 eigrp topology

IPv6-EIGRP Topology Table for AS(1)/ID(2001:0DB8:10::/64)

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

P 2001:0DB8:3::/64, 1 successors, FD is 281600
via Connected, Ethernet1/0
```

The EIGRP neighbors are shown in Example 3-22.
Example 3-22  Verifying EIGRP Neighbors

IPv6-router# show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H   Address                Interface   Hold   Uptime   SRTT    RTO    Q     Seq (sec)           (ms)          Cnt    Num
0   Link-local address:    Se0/0      13  15:17:58   44    264    0      12  FE80::2

Example 3-23 displays the associated routing table.

Example 3-23  Verifying the Routing Table

IPv6-router# show ipv6 route eigrp
IPv6 Routing Table - 12 entries
Codes:  C - Connected,  L - Local,  S - Static,  R - RIP,  B - BGP
       U - Per-user Static route,  M - MIPv6
       I1 - ISIS L1,  I2 - ISIS L2,  IA - ISIS interarea,  IS - ISIS summary
       O - OSPF intra,  OI - OSPF inter,  OE1 - OSPF ext 1,  OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1,  ON2 - OSPF NSSA ext 2
       D - EIGRP,  EX - EIGRP external
D   1000:AB8::/64 [90/2297856] via FE80::2, Serial0/0
D   2000:AB8::/64 [90/2297856] via FE80::2, Serial0/0
D   3000:AB8::/64 [90/2297856] via FE80::2, Serial0/0

The show commands in Example 3-20 through Example 3-23 have the same role as in EIGRP for IPv4. The differences are related to the protocol output:

- To display entries in the EIGRP for IPv6 topology table, use the show ipv6 eigrp topology command in privileged EXEC mode.
- To display the neighbors discovered by EIGRP for IPv6, use the show ipv6 eigrp neighbors command.
- The show ipv6 route eigrp command reveals the content of the IPv6 routing table that includes the routes specific to EIGRP.
EIGRP for IPv6 Configuration Example

Figure 3-20 along with the configurations in Examples 3-24 and 3-25 provide a simple two-node network with a Branch router and an HQ router.

![IPv6 EIGRP AS 100]

**Figure 3-20**  Two-Router IPv6 Network

On the Branch router, EIGRP for IPv6 is enabled with AS 100. EIGRP is then enabled on the interface GigabitEthernet0/1.

**Example 3-24  Branch Router Configuration**

```bash
Branch(config)# ipv6 router eigrp 100
Branch(config-router)# no shutdown
Branch(config-router)# exit
Branch(config)# interface GigabitEthernet0/1
Branch(config-if)# ipv6 eigrp 100
```

As displayed in Example 3-25, on the HQ router, first EIGRP for IPv6 is enabled with AS 100. Then interfaces GigabitEthernet0/0 and GigabitEthernet0/1 are enabled for IPv6 EIGRP.

**Example 3-25  HQ Router Configuration**

```bash
HQ(config)# ipv6 router eigrp 100
HQ(config-router)# no shutdown
HQ(config)# exit
HQ(config)# interface GigabitEthernet0/0
HQ(config-if)# ipv6 eigrp 100
HQ(config-if)# exit
HQ(config)# interface GigabitEthernet0/1
HQ(config-if)# ipv6 eigrp 100
```

In the `show ipv6 eigrp interfaces` command output that follows in Example 3-26 for the Branch router, one neighbor is on the GigabitEthernet0/1 interface, which is the only interface that is included in the EIGRP process.
**Example 3-26  Verifying EIGRP Interface**

Branch# `show ipv6 eigrp interfaces`
IPv6-EIGRP interfaces for AS(100)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Peers</th>
<th>Xmit Queue Un/Reliable</th>
<th>Mean SRTT Un/Reliable</th>
<th>Pacing Time</th>
<th>Multicast Flow Timer</th>
<th>Pending Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>1</td>
<td>0/0</td>
<td>0</td>
<td>0/10</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Authentication mode is not set

Example 3-27 shows the output of the `show ipv6 eigrp neighbors` command from the Branch router. The fields in the command output are described in Table 3-7.

**Example 3-27  Reviewing EIGRP Neighbors**

IPv6-router# `show ipv6 eigrp neighbors`
IPv6-EIGRP neighbors for process 1

<table>
<thead>
<tr>
<th>H</th>
<th>Address</th>
<th>Interface</th>
<th>Hold (sec)</th>
<th>Uptime (ms)</th>
<th>SRTT</th>
<th>RTO</th>
<th>Q</th>
<th>Seq</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Link-local address:</td>
<td>Gi0/1</td>
<td>12</td>
<td>00:20:48</td>
<td>9</td>
<td>100</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>FE80::FE99:47FF:FEE5:2671</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 3-7  Significant Fields in the `show ipv6 eigrp neighbors` Command from the Branch Router**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-local address</td>
<td>The IPv6 interface address used for communication local to a single subnet only. Link-local packets are not routed. EIGRP IPv6 uses this to establish neighbor relationships.</td>
</tr>
<tr>
<td>Interface</td>
<td>The EIGRP interface.</td>
</tr>
<tr>
<td>Hold</td>
<td>The amount of time an EIGRP neighbor awaits a hello packet from a neighbor before determining that the neighbor relationship should be timed out and broken. The default is three times the hold timer.</td>
</tr>
<tr>
<td>Uptime</td>
<td>How long the neighbor relationship has been established.</td>
</tr>
</tbody>
</table>

The `show ipv6 eigrp topology` command displays the topology table of EIGRP for IPv6 routes, as demonstrated in Example 3-28. All the routes are present in the topology table, but only the best ones are in the routing table.
Example 3-28  IPv6 Topology

<table>
<thead>
<tr>
<th>Branch#</th>
<th>show ipv6 eigrp topology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EIGRP-IPv6 Topology Table for AS(100)/ID(209.165.201.1)</td>
</tr>
<tr>
<td>Codes:</td>
<td>P - Passive, A - Active, U - Update, Q - Query, R - Reply,</td>
</tr>
<tr>
<td></td>
<td>r - reply Status, s - sia Status</td>
</tr>
<tr>
<td></td>
<td>P 2001:DB8:D1A5:C900::/64, 1 successors, FD is 28160</td>
</tr>
<tr>
<td></td>
<td>via Connected, GigabitEthernet0/1</td>
</tr>
<tr>
<td></td>
<td>P 2001:DB8:AC10:100::/64, 1 successors, FD is 156160</td>
</tr>
<tr>
<td></td>
<td>via FE80::FE99:47FF:FEE5:2671 (156160/128256), GigabitEthernet0/1</td>
</tr>
</tbody>
</table>

Example 3-29 displays output from the `show ipv6 route eigrp` command. Here, you are presented with a route that is learned by the EIGRP routing protocol.

Example 3-29  Verifying the EIGRP Routes in the Routing Table

<table>
<thead>
<tr>
<th>Branch#</th>
<th>show ipv6 route eigrp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPv6 Routing Table - default - 4 entries</td>
</tr>
<tr>
<td>Codes:</td>
<td>C - Connected, L - Local, S - Static, U - Per-user Static route</td>
</tr>
<tr>
<td></td>
<td>B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2</td>
</tr>
<tr>
<td></td>
<td>IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external</td>
</tr>
<tr>
<td></td>
<td>ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr – Redirect</td>
</tr>
<tr>
<td></td>
<td>O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2</td>
</tr>
<tr>
<td></td>
<td>ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2</td>
</tr>
<tr>
<td>D</td>
<td>2001:DB8:AC10:100::/64 [90/156160]</td>
</tr>
<tr>
<td></td>
<td>via FE80::FE99:47FF:FEE5:2671, GigabitEthernet0/1</td>
</tr>
</tbody>
</table>

Troubleshooting EIGRP for IPv6

When considering EIGRP for IPv6, there are many similarities to EIGRP for IPv4. The commands are comparable, the algorithm is the same, and the metrics work alike. However, being aware of some of the major differences and key points makes troubleshooting easier. The following points provide a brief summary:

- EIGRP for IPv6 is directly designed on the interfaces over which it runs. This feature allows EIGRP for IPv6 to be configured without the use of a global IPv6 address. There is no network statement in EIGRP for IPv6.
- In per-interface design at system startup, if EIGRP has been configured on an interface, then the EIGRP protocol may start running before any EIGRP router mode commands have been executed.
- An EIGRP for IPv6 protocol instance requires a router ID before it can start running.
- EIGRP for IPv6 has a shutdown feature. The routing process should be in **no shutdown** mode in order to start running.

- When using a passive-interface configuration, EIGRP for IPv6 does not need to be configured on the interface that is made passive.

- EIGRP for IPv6 provides route filtering using the **distribute-list** command.

**Note**  As with IPv4 EIGRP, distribute lists are explored in more detail in the Implementing Cisco IP Routing (ROUTE) course and the related texts for preparation for the Implementing Cisco IP Routing (ROUTE) exam.

**Chapter Summary**

Dynamic routing protocols are defined by type, distance vector or link state. Distance vector protocols use a metric to determine the path through the network on a hop-by-hop basis. Link-state protocols keep a topology of all routers and links in the network. Examples of distance vector protocols are EIGRP and RIP. Examples of link-state protocols are OSPF and BGP.

Dynamic routing protocols are classified as Exterior Gateway Protocol (EGP) or Interior Gateway Protocol (IGP). An EGP is used between different autonomous systems, such as autonomous systems connected to the public Internet. IGPs are used inside a network. The only current EGP for IPv4 and IPv6 is BGP. Examples of IGPs are OSPF, EIGRP, and RIP.

EIGRP is an IGP that is considered an advanced distance vector protocol because it has many added features, such as partial updates. EIGRP uses the DUAL algorithm for its topology and metric calculations. It is suitable for many network designs. It supports multiple protocols through separate processes, called protocol-dependent modules.

EIGRP for IPv4 and EIGRP for IPv6 have very similar operating models, such as configuration and troubleshooting. The main deviations are where IPv4 and IPv6 differ as protocols. The primary differences are that IPv6 uses link-local addressing for EIGRP (IPv6) neighbor establishment; EIGRP for IPv6 is configured on an interface-by-interface basis; and the creation of passive interfaces in IPv6 is done not by configuring an interface but by adding configuration for the passive interface.
Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are located in Appendix A, “Answers to Chapter Review Questions.”

1. In which two ways does the configuration of EIGRP on IPv6 differ from the configuration of EIGRP on IPv4? (Choose two.) (Source: “EIGRP for IPv6 Command Syntax”)
   a. The network command is changed into the ipv6 network command for EIGRP for IPv6.
   b. EIGRP for IPv6 can only be explicitly enabled with the no shutdown command. There is no network command.
   c. EIGRP for IPv6 is configured per interface on Cisco routers.
   d. If you run EIGRP for IPv6, you have to run EIGRP for IPv4; but if you run EIGRP for IPv4, you do not need to run EIGRP for IPv6.

2. Which command can you use to show if EIGRP for IPv6 is running? (Source: “EIGRP for IPv6 Command Syntax”)
   a. show ipv6 interface
   b. show ipv6 protocol
   c. show ipv6 eigrp dual
   d. show eigrp ipv6 dual

3. Which is not a valid IPv6 EIGRP command? (Source: EIGRP Basic Configuration)
   a. show ipv6 eigrp topology
   b. show ipv6 route eigrp
   c. show ipv6 eigrp status
   d. show ipv6 eigrp interfaces

4. Which of the following applies to EIGRP AS numbers? (Source: “Troubleshooting EIGRP Neighbor Issues”)
   a. Need to match between EIGRP neighbors only
   b. Need to match OSPF area numbers if routes are being redistributed
   c. Need to match between all EIGRP routers in the topology
   d. Don't need to match at all
   e. Must match BGP AS numbers

5. Which command is most useful for determining if an EIGRP neighbor relationship is not established due to a connectivity issue? (Source: “Troubleshooting EIGRP Neighbor Issues”)
   a. show ip protocols
   b. show ip eigrp neighbors
   c. show eigrp topology
   d. show ip protocols
   e. show ip interfaces brief
6. Which of the following applies to an EIGRP passive interface? (Source: “Troubleshooting EIGRP Neighbor Issues”)
   a. Only makes a neighbor relationship if a neighbor that is on a directly connected subnet initiates the connection
   b. Can be seen by the `show ip eigrp passive-interfaces` command
   c. Can be seen by the `show ip protocols` command
   d. Can have a different AS number assigned to it

7. Route filtering can be done on which of the following? (Source: “Issues Caused by Route Filtering”)
   a. Inbound routes only
   b. Outbound routes only
   c. Either inbound or outbound routes

8. Where is automatic summarization performed? (Source: Classful Routing Versus Classless Routing)
   a. At any contiguous network block
   b. At classful network boundaries
   c. Can be performed on the same classful boundary on more than one network segment at the same time
   d. At the intersection of the classful and classless routing protocol.

9. Which command correctly specifies that network 10.0.0.0 is directly connected to a router that is running EIGRP and should be advertised? (Source: “Implementing EIGRP for IPv6”)
   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`

10. Connect each EIGRP feature on the left with its description on the right. (Source: “Implementing EIGRP for IPv6”)
    1. Reduced bandwidth usage  a. EIGRP algorithm by which EIGRP achieves rapid convergence
    2. Classless routing    b. A direct consequence of using partial updates
    3. Load balancing    c. EIGRP knows two types: equal and unequal
    4. DUAL    d. Routing mask is advertised for each destination network
11. Which two criteria does EIGRP use by default to calculate its metric? (Choose two.) (Source: “Implementing EIGRP for IPv6”)
   a. Bandwidth
   b. Reliability
   c. Load
   d. MTU
   e. Delay

12. Connect each term on the left to its description on the right. (Source: “Implementing EIGRP for IPv6”)
   1. Feasible distance  
      a. The best EIGRP metric for an EIGRP neighbor to reach a particular network
   2. Advertised distance  
      b. The end-to-end metric that is transmitted from the router for a remote network
   3. Administrative distance  
      c. The end-to-end EIGRP metric from a router to reach a particular network
   4. Composite metric  
      d. Used to rate the trustworthiness of each routing information source

13. Which letter is used to signify that a route in the show ip routes command originates from EIGRP? (Source: “Verification of EIGRP Configuration and Operation”)
   a. A
   b. D
   c. E
   d. L

14. Which is not a valid command? (Source: “Verification of EIGRP Configuration and Operation”)
   a. show ip eigrp dual process as_number
   b. show ip eigrp interfaces
   c. show ip route
   d. show ip eigrp neighbors

15. All routing protocols support uneven-cost load balancing. True or False? (Source: “Load Balancing with EIGRP”)
16. Which interface(s) on the Branch router does not have an EIGRP neighbor? (Source: “Verification of EIGRP Configuration and Operation”)
   a. Gigabit0/0
   b. Gigabit0/1
   c. Gigabit0/2
   d. Gigabit0/3
   e. All interfaces have an EIGRP neighbor
   f. No interfaces have an EIGRP neighbor

17. Which two choices are not a characteristic of EIGRP? (Source: “Dynamic Routing Overview”)
   a. Determines distance to any destination in the network
   b. Uses an algorithm called DUAL
   c. Uses an algorithm called SPF
   d. Has a map of every destination in the network

18. Which command would you use to investigate which interfaces are enabled for the EIGRP routing process? (Source: “Troubleshooting EIGRP Neighbor Issues”)
   a. show ip eigrp interfaces
   b. show ip eigrp neighbors
   c. show ip interfaces brief
   d. show eigrp enabled interfaces
19. Which of the following statements are false? (Source: “Troubleshooting EIGRP for IPv6”)

   a. In per-interface configuration at system startup, if IPv6 EIGRP has been configured on an interface, then the IPv6 EIGRP protocol may start running before any EIGRP router mode commands have been executed.
   b. An EIGRP for IPv6 protocol instance does not need a router ID before it can start running. The router ID can be added later.
   c. When using a passive-interface configuration, EIGRP for IPv6 does not need to be configured on the interface that is made passive.
   d. EIGRP for IPv6 is not directly configured on the interfaces over which it runs. In the network statement in EIGRP for IPv6, the interface must be explicitly defined.
   e. EIGRP for IPv6 has a shutdown feature. The routing process must be in no shutdown mode in order to start running.
   f. EIGRP for IPv6 provides route filtering using the distribute-list prefix-list command. Use of the route-map command is not supported for route filtering with a distribute list.
   g. EIGRP uses the advanced DUAL algorithm that maintains a database of every node on the network.

20. Which is not a basic component of EIGRP? (Source: “EIGRP Features and Function”)

   a. Topology database
   b. DUAL algorithm
   c. Protocol-dependent modules
   d. Hello packets

21. Which is not a valid dynamic routing protocol classification? (Source: “Dynamic Routing Protocols”)

   a. Hybrid
   b. Distance vector
   c. Link state

22. Connect each term on the left with its definition on the right. (Source: “Dynamic Routing Review”)

   1. Distance vector protocol a. Keeps track of all links and routers in the network
   2. EGP b. Internal routing for a single routing domain
   3. Link-state protocol c. Tracks the network path on a hop-by-hop basis
   4. IGP d. Connects routing domains
This page intentionally left blank
SYMBOLES

% (percent sign), 83
. (dot), 54
: (colons), 75

A

aborted transmissions, 62
ABRs (Area Boundary Routers), 152
abstraction, platform, 330
access
CE (Customer Edge) routers, 264
local access rates, 235
MIBs (Management Information Bases), 275
NADs (network access devices), 195
remote-access VPNs, 253
SNMP (Simple Network Management Protocol), 276
WANs (wide-area networks), 194
access control lists. See ACLs
access servers, CDP (Cisco Discovery Protocol), 58
ACLs (access control lists)
counters, reviewing, 355
debugging, triggering, 351-356
filtering, 122
IPv4 (Internet Protocol version 4), 50, 71-72
IPv6 (Internet Protocol version 6), 84-86
OSPF (Open Shortest Path First), 167
SNMP (Simple Network Management Protocol), 279
validation, 353
ACs (attachment circuits), 263
activating PPP (Point-to-Point Protocol) links, 221
active routers, 37
AD (advertised distance), 102
Adaptive Security Appliance. See ASAs
adding VLANs (virtual LANs), 5

Address Resolution Protocol. See ARP

addresses
- Frame Relay, mapping, 240-243
- IP (Internet Protocol), DRs/BDRs, 149
- IPv6 (Internet Protocol version 6), troubleshooting, 75-76
- MAC (Media Access Control), 10, 23, 58
  unicast, troubleshooting, 76-77

adjacencies, neighbors, 147-149

administrative distance, routing protocols, 95-98

advantages of link-state routing protocols, 144

advertised distance. See AD

advertisements
- EIGRP (Enhanced Interior Gateway Protocol), 126
- LSAs (link-state advertisements), 144-145
  verification, 172

agents, SNMP (Simple Network Management Protocol), 270. See also SNMP
  obtaining data from, 271
  sending data to, 274

aggregation, NetFlow, 285

algorithms
- DUAL, 99, 125
  dynamic routing, 92
- SPF (shortest path first), 94, 145

analog phone line interfaces, 201

analyzing STP (Spanning Tree Protocol), 24-26

Antireplay protection, 256

applications. See also tools
- Cisco IOS. See IOS
- hypervisor, 72-74
- point-to-point networks, 191
- Telnet, 55
- terminal-emulation program, 346
- WAAS (Wide Area Application Services), 300

applying
- ACLs (access control lists), 71
  Output Interpreter, 341

architecture
- CRS (Carrier Routing System), 291
- NetFlow, 285-286
- redundancy, 12
- WANs (wide-area networks), 188

Area Boundary Routers. See ABRs

areas
- IDs, 148
- NSSAs (not-so-stubby areas), 156
- OSPF (Open Shortest Path First)
  structures, 150
  types, 150-153
  stub, 155-156
  totally stub, 157

ARP (Address Resolution Protocol), 51, 57
  caches, 290
  inverse, 236

AS (autonomous systems), 92, 119

ASAs (Adaptive Security Appliance), 253

ASBRs (Autonomous System Boundary Routers), 152-153
ATM (Asynchronous Transfer Mode), 198
attachment circuits. See ACs
Attempt state, 166
authentication
CHAP (Challenge-Handshake Authentication Protocol), 222-223, 359
EIGRP (Enhanced Interior Gateway Protocol), 114-115
IPSec, 256
OSPF (Open Shortest Path First), 149
PAP (Password Authentication Protocol), 222
SNMP (Simple Network Management Protocol), 271
autoconfiguration, 301
automatic network summarization, 123
automatic trunk negotiation, 8
Autonomous System Boundary Routers. See ASBRs
autonomous systems. See AS
auto-summary command, 124
avoidance, loops, 13

bandwidth
EIGRP (Enhanced Interior Gateway Protocol), 103
metrics, 126
reduced bandwidth usage, 99
redundancy, 29-35
references
modification, 147
verification, 176
serial interfaces, 212
bandwidth bandwidth_kbps command, 224
bandwidth bandwidth_kilobits command, 213
Barker, Keith, 72
basic connectivity, testing, 51
BDRs (backup designated routers), 149
BGP (Border Gateway Protocol), 93, 128
bidirectional communication, 147-148
BIDs (bridge IDs), 14, 17, 22
blocking ports, 14
booting routers, 292-293, 302
bootstrap code, 292, 295
Border Gateway Protocol. See BGP
BPDU Guard, 28
BPDUs (bridge protocol data units), 13, 16, 21
Branch Routers
EIGRP (Enhanced Interior Gateway Protocol)
configuration, 105
IPv6 configuration, 133
Frame Relay configuration, 248
GRE tunnel configurations, 259
OSPFv3 (Open Shortest Path First version 3), 178
point-to-multipoint configuration, 248
point-to-point Frame Relay, 246
SNMP configuration, 278
Break key emulation, 314
bridge IDs. See BIDs
Bridge Priority field, 23
bridge protocol data units. See BPDUs
bridging loops, 18, 26
broadband, 198
broadcasts
replication, 238
storms, 13
buffers, packets, 290
Bug Toolkit, 344
building
LSDBs (links-state databases), 149-150
redundant switches topologies, 11

C

cablelength command, 217
cables. See also connections
crossover, 196, 209
Ethernet, 199
fiber optic, 187-207
modems, 194, 202
serial, 195
troubleshooting, 50
caches
ARP (Address Resolution Protocol)
RAM (random-access memory), 290
viewing, 57
memory, 290
calculations, metrics, 128
CAPEX (capital expenditure), 193
Carrier Routing System. See CRS
carrier transitions, 61
CDP (Cisco Discovery Protocol), 13, 58-60
CE (Customer Edge) routers, 262
central processing units. See CPUs
Challenge-Handshake Authentication Protocol. See CHAP
channel-group channel-no timeslots
timeslot-list speed command, 217
channel service unit/data service unit. See CSU/DSU
channels, viewing ports, 35
CHAP (Challenge-Handshake Authentication Protocol), 198, 222-223, 359
configuration, 227
PPP (Point-to-Point Protocol), 225-227
character output, ping command, 54
checking routing for networks output, 120
CIDR (classless interdomain routing), 76
CIR (committed information rate), 235
circuit-switched communication links, 204
commands  407

Circuits
   ACs (attachment circuits), 263
   T1/E1, 200-201
Cisco Discovery Protocol. See CDP
Cisco Feature Navigator, 308
Cisco IOS File System. See IFS
Cisco IOS Software. See IOS
Cisco IOS-XE, 330
Cisco IOS-XR, 329-330
Cisco License Manager. See CLM
Cisco Licenses Registration Portal, 318
Cisco NX-OS, 331
Cisco Prime Infrastructure, 270
Cisco Unified Border Element. See CUBE
Cisco Virtual Office. See CVO
Claim Certificates, 316
classful routing, 94-95
classification of routing protocols, 93
classless interdomain routing. See CIDR
classless routing, 94-95, 99
CLE (Common Language Equipment), 319
clientless VPNs (virtual private networks), 206
CLM (Cisco License Manager), 318
clockrate clock_rate_bits command, 213
clockrate clock_rate_bps command, 224
codes
   bootstrap, 292, 295
   IPv6 neighbor discovery table, 82
collecting IOS device diagnostic information, 340-341
Collector (NetFlow), 283
collisions, 61
colons (:), 75
commands
   auto-summary, 124
   bandwidth
      bandwidth_kbps, 224
      bandwidth_kilobits, 213
cablelength, 217
   channel-group channel-no timeslots
timeslot-list speed, 217
clockrate
   clock_rate_bits, 213
clock_rate_bps, 224
controller type slot/port, 217
copy, 304
debug, 352
debug ip packet, 348, 352
EIGRP (Enhanced Interior Gateway Protocol), 105, 130-131
encapsulation
   frame-relay, 246, 249
   ppp, 224, 227
encapsulation frame-relay
   [cisco | ietf], 244
EXEC, 302
frame-relay
   interface dlcid lci, 244-246
   lmi, 250
   map, 252
   map protocol protocol_address
dlcid, 244-246, 249
   pvc, 251
framing framing_type, 217
GET, 274
hostname hostname, 227
interface
  interface, 244
  interface.subinterface point-to-multipoint, 249
  interface.subinterface point-to-point, 246
  serial interface_number, 213
  serial port/mod, 224, 227
  tunnel<tunnel_number>, 259
ip address
  ip_address subnet_mask, 244
  ip_v4_address subnet_mask, 224, 227
ip default-network, 67
ip flow, 287
ip flow-export
  destination ip-address udp-port, 287
  version version, 287
ip host name ip_address, 69
ip ospf
  cost cost, 160
  process_id area-id area_id, 170
ipv6
  router ospf process-id, 179
  router ospf process-id area area_id, 179
license boot module, 323
linecode code_type, 217
netsh interface ipv6 show neighbor Windows, 80
network-clock-select priority t1_or_e1 slot/port, 217
network network wildcard_mask
  area area_id, 160
no debug, 350
no shutdown, 213, 224
OSPFv3 (Open Shortest Path First version 3), 179
passive-interface interface, 171
ping, 51
  EIGRP (Enhanced Interior Gateway Protocol), 118
  extended, 53
  IPv6 (Internet Protocol version 6), 79
  output characters, 54
  static name resolution, 69
  triggering ACL (access control list) debugging, 355
  troubleshooting ACLs (access control lists), 72
ppp authentication chap, 227
redistribute, 153
reload, 320
router-id router_id, 179
router ospf process_id, 160
serial interfaces, 213
SET, 274
show
  access-lists, 71
  buffers, 340
  cdp neighbors, 59
  controllers, 340
  debug, 350
  etherchannel port-channel, 35
  etherchannel summary, 34
  flash0:, 306
  glbp, 41
  interface, 60, 104, 340
  interface interface switchport,
interface port-channel, 34
interfaces, 7, 62, 249
ip cache flow, 288
destination ip_address, 259
ip eigrp neighbors, 106-107
mode gre ip, 259
ip eigrp topology, 110-111
source ip_address, 259
ip flow interface, 287
switchport
ip interface, 168, 260
nonegotiate interface, 9
ip interface brief, 260
terminal monitor, 346
ip ospf interface, 170, 175
traceroute, 51
tunnel
ip ospf neighbor, 172
tracert, 52
ip protocols, 120, 170
undebbug, 350
ip route, 63-65, 108-109, 173
username username password password, 227
ipv6 eigrp neighbors, 134
vlan
license, 320, 340
global configuration, 4
license udi, 319
vlan_id, 10
mac address-table, 58
committed information rate. See CIR
process cpu, 340
Common Language Equipment. See CLE
processes memory, 340
Common Spanning Tree. See CST
running-config, 302, 340
components
snmp additional_options, 278
BPDUs (bridge protocol data units), 16
spanning-tree, 25
EIGRP (Enhanced Interior Gateway Protocol), 99, 115-118
stacks, 340
end-to-end IPv4 (Internet Protocol version 4), 48-50
startup-config, 302
end-to-end IPv6 (Internet Protocol version 6), 78-80
techn, 341
IFS (Cisco IOS File System), 303
version, 298, 321, 340
Interface and Hardware Component
vlans, 5
Configuration Guide,
shutdown, 227
username
snmp-server
chassis-id serial_no, 278
community string [RO | RQ], 278
contact contact_name, 278
host ip_address trap
community_string, 278
location location, 278
confidentiality, 256, 271
configuration

ABRs (Area Boundary Routers), 153
ACLs (access control lists), 71
CHAP (Challenge-Handshake Authentication Protocol), 227
Cisco IOS, 300-302
EIGRP (Enhanced Interior Gateway Protocol), 105-106
- authentication, 114-115
- IPv6 (Internet Protocol version 6), 133-135
- verification, 106-108
EtherChannel, 33-34
file management, 311-313
GRE (Generic Routing Encapsulation) tunnels, 256-261
hypervisor, 74
integrated CSU/DSU, 215-216
IOS traps, 273
L3VPN (Layer 3 VPN), 369-372
merging, 312
multilink PPP (Point-to-Point Protocol) over serial lines, 228-232
NetFlow, 286-287
network device management, 270
NMS (Network Management System), 272
OSPF (Open Shortest Path First), multiarea IPv4 implementation, 158-160
OSPFv3 (Open Shortest Path First version 3), 178-179
point-to-multipoint, 247-249
PPP (Point-to-Point Protocol), 223-227
registers, 291-295

routers
- backbones, 151
- normal areas, 151
running configuration files, 290
serial interfaces, WANs, 209-214
SNMP (Simple Network Management Protocol), 276-279
switches, 4
syslog, 281
trunks, 7
VLANs (virtual LANs), 3
WANs (wide-area networks), 243-244, 249-252

congestion, troubleshooting, 61
connections
- basic connectivity, testing, 51
- CPE (customer premises equipment), 194
- Frame Relay, 185, 198
- IPv4 (Internet Protocol version 4)
  - CDP (Cisco Discovery Protocol), 58-60
  - troubleshooting, 48
  - verifying, 51-58
- IPv6 (Internet Protocol version 6), 78-80
- Layer 3, 63
- physical connection issues, 60-63
- routing domains, 93
- switch-to-switch connectivity, 6
- troubleshooting, 47
- WANs (wide-area networks), 187

consoles, CDP (Cisco Discovery Protocol) messages, 60
controller type slot/port command, 217
debugging

conventions, IPv6 (Internet Protocol version 6) addresses, 75-76
convergence
distance vector protocols, 94
rapid, 99
STP (Spanning Tree Protocol), 21
converting optical fiber, 194
copy command, 304
copy tftp running-config command,
core routers, WANs (wide-area networks), 193
costs
interfaces, 175
OSPF (Open Shortest Path First) modification, 147
counters, reviewing ACLs (access control lists), 355
CPE (customer premises equipment), 193
CPUs (central processing units), 290
Crashes, 340. See also troubleshooting
CRC (cyclic redundancy check), 61
crossover cables, 196, 209
CRS (Carrier Routing System), 291
CST (Common Spanning Tree), 20
CSU/DSU (channel service unit/data service unit), 61, 212
  integrated CSU/DSU
    back-to-back routers, 216-209
    configuration, 215-216
  integrated modules, 214
  WANs (wide-area networks), 192-193
CUBE (Cisco Unified Border Element), 40
current paths, identification of, 63-66

Customer Edge. See CE
customer logical WANs, 263
customer networks, 262
customer premises equipment. See CPE
CVO (Cisco Virtual Office), 205
cyclic redundancy check. See CRC

data centers, troubleshooting, 86
data circuit-terminating equipment. See DCE
data integrity, 256
data-link connection identifiers. See DLCIs
data structures, link-state routing protocols, 145-146
data terminal equipment. See DTE
database descriptors. See DBDs
databases
  LSDBs (links-state databases), 144, 145
  MAC (Media Access Control), 13
  VLANs (virtual LANs), 5
DBDs (database descriptors), 149, 164
DCE (data circuit-terminating equipment), 193, 196, 213
dead intervals, 148
debug command, 352
debug ip packet command, 348, 352
debugging
devices, 345
capturing output, 345-350
conditionally triggered, 356-357
limiting output, 351
protocol operations, 359-361
triggering ACLs (access control lists), 351-356
troubleshooting, 357-359
verification, 350-351
IP (Internet Protocol) packets, 350
dedicated communication links, 204
dedicated link extranets, 211
default administrative distances, 96
default configuration, switches, 4
default gateways,
  IPv4 (Internet Protocol version 4), 66
  IPv6 (Internet Protocol version 6), 81-83
  redundancy, 36-41
defects, researching IOS, 343-345
delay
  EIGRP (Enhanced Interior Gateway Protocol), 103
  metrics, 126
  polling data, monitoring in SNMP, 272
DELAY code, 82
deployment
  HSRP (Hot Standby Router Protocol), 39-40
  VPNs (virtual private networks), 252
description message, 281
designated port. See DP
designated routers. See DRs
desired paths, identification of, 63-66
destination networks, path selection, 146
detection, applying Output Interpreter, 341
devices, 269. See also network device management
debugging, 345
capturing output, 345-350
conditionally triggered, 356-357
limiting output, 351
protocol operations, 359-361
triggering ACLs (access control lists), 351-356
troubleshooting, 357-359
verification, 350-351
IOS, collecting diagnostic information, 340-341
IPSec (IP Security), 255-256
NADs (network access devices), 195
UDIs (universal device identifiers), 319
VLANs (virtual LANs), 2. See also VLANs
VoIP (Voice over IP), 58
WANs (wide-area networks), 192-195
diagnostics. See also troubleshooting
device information, collecting IOS, 340-341
  routers, 340
digital subscriber line. See DSL
disabling
  automatic summarization, 124
debugging, 350-351
  ports, 14
disadvantages of link-state routing protocols, 153
discovery, neighbors, 238
distance vector protocols, 93
EIGRP (Enhanced Interior Gateway Protocol)  413

distances
  AD (advertised distance), 102
  administrative, routing protocols, 95-98
  FD (feasible distance), 102
distribute lists, filtering, 122
DLCIs (data-link connection identifiers), 235
DNS (Domain Name Server), 50
  dynamic name resolution, 69
  hostname validation, 55
  lookup, 69
  troubleshooting, 68
domains
  classful routing, 95
  routing, 92
dot (.), 54
Down state, 166
DP (designated port), 14, 19
drops, queues, 60
DRs (designated routers), 149
DSL (digital subscriber line), 198
  modems, 193
  termination, 201
DTE (data terminal equipment), 193, 196, 213
DTP (Dynamic Trunking Protocol), 8-9
DUAL algorithm, 99, 125
dynamic name resolution, 69-71
dynamic routing, overview of, 92-106
Dynamic Trunking Protocol. See DTP

E

echo requests (ICMP), 51
EGP (Exterior Gateway Protocol), 93
EIA/TIA-232 interfaces, 195
EIGRP (Enhanced Interior Gateway Protocol), 91
  authentication, 114-115
  configuration, 105-108
  dynamic routing, 92-106
  features, 98-115
  interfaces, enabling, 120
IPv6 (Internet Protocol version 6)
  command syntax, 130-131
  configuration, 133-135
  feasible successors, 128-129
  implementation, 124-136
  load balancing, 129
  theory of operation, 124
  troubleshooting, 135
  verification, 131-132
load balancing, 110-112
metrics, 103-104, 126
neighbors, 118-121, 134
packet types, 100-101
passive interfaces, 108-111
path selection, 101, 126
traffic sharing, 113-114
troubleshooting, 115-124
  automatic network summarization, 123
  components, 115-118
  route filtering, 122-124
routing tables, 121
unadvertised routes, 121

variance, 112-113

emulation
Break key, 314
terminal-emulation program, 346

enabling
debugging, 348
EIGRP (Enhanced Interior Gateway Protocol) interfaces, 120

encapsulation
GRE (Generic Routing Encapsulation), 256-261
serial lines, 219

encapsulation frame-relay
[cisco | ietf] command, 244

encapsulation frame-relay command, 246, 249

encapsulation ppp command, 224, 227

encryption, 256

end-to-end connections
IPv4 (Internet Protocol version 4)
components, 48-50
IPv6 (Internet Protocol version 6)
components, 78-80

End User License Agreement. See EULA

Enhanced Interior Gateway Protocol. See EIGRP

entries, troubleshooting inaccurate routing, 124

environments, virtual
IPv4 (Internet Protocol version 4), 72-74
IPv6 (Internet Protocol version 6), 86
environments, virtual
IPv4 (Internet Protocol version 4), 72-74
IPv6 (Internet Protocol version 6), 86

errors
CRC (cyclic redundancy check), 61
Ethernet, 62
framing, 62
input, 61
user-reported, 49

EtherChannel
bandwidth, increasing, 29-35
configuration, 33-34
protocols, 31

LACP (Link Aggregation Control Protocol), 32-33
PAgP (Port Aggregation Protocol), 31-32

verification, 34-35

Ethernet, 198
cable, 199
crossover cables, 196
interfaces, trunks, 6
links, troubleshooting, 62
Metro, 209

EULA (End User License Agreement), 316
evaluation license installation,
273-322
exchange protocols, 164
exchange state, 166
EXEC command, 302
EXEC mode, 314, 341
exstart state, 166
extended ping, 53
Extended System ID field, 23
extensibility (Cisco NX-OS), 331
Exterior Gateway Protocol. See EGP
extranets, 209
functions of WANs (wide-area networks)  415

F

facility message, 281
failures. See also troubleshooting
   link-state routing protocols, 144
   STP (Spanning Tree Protocol), 26-28
FD (feasible distance), 102
feasible successors, 128-129
features of EIGRP (Enhanced Interior
   Gateway Protocol), 98-115
fiber optic cabling, 207-187
filenames, interpreting Cisco IOS
   images, 305-306
files
   configuration, managing, 311-313
   repositories, 304
   running configuration, 290
filters
   BPDUs (bridge protocol data units),  
      21
   NetFlow, 285
   routes, troubleshooting EIGRP,  
      122-124
flash memory, 290, 303
Flexible NetFlow. See NetFlow
flow
   control, Layer 2, 197
   interfaces, NetFlow, 287
   messages, CHAP, 222
   SFTP (Secure File Transfer Protocol),  
      274
flowcharts, troubleshooting EIGRP,  
   115
formatting. See also configuration
   IPv6 (Internet Protocol version 6)
      addresses, 56-76
   syslog messages, 281

Frame Relay
   connections, 185, 198
   WANs (wide-area networks), 233
      configuration, 243-244
      mapping addresses, 240-243
      overview of, 233-236
      point-to-multipoint configuration, 247-249
      point-to-point subinterface
         configuration, 245-246
      signaling, 239-240
      topologies, 236-237
      troubleshooting, 237-239
      verifying configuration,  
         249-252
frame-relay interface dlci dlci command, 244-246
frame-relay lmi command, 250
frame-relay map command, 252
frame-relay map protocol protocol-address dlci command, 244-246,  
   249
frame-relay pvc command, 251
frames, multiple frame transmission,  
   13
framing errors, 62
framing framing_type command, 217
FTP (File Transfer Protocol), 303
full-mesh networks
   Frame Relay, 236
   WANs (wide-area networks),  
      189-191
full state, 166
functions of WANs (wide-area networks), 186
Gateway Load-Balancing Protocol.
See GLBP
gateways, default
  IPv4 (Internet Protocol version 4), 66
  IPv6 (Internet Protocol version 6), 81-83
  redundancy, 36-41
Generic Routing Encapsulation. See GRE
GET command, 274
GLBP (Gateway Load-Balancing Protocol), 40-41
global key chains, 115
global unicast addresses, 76
GRE (Generic Routing Encapsulation), 256-261
groups, standby, 37
guards, BPDUs (bridge protocol data units), 21
HDLC (High-Level Data Link Control) protocol, 197, 218-220
Hello
  intervals, 148
  protocol, 163
hierarchies, link-state routing protocols, 150
High-Level Data Link Control protocol. See HDLC protocol
hops, 94
hostname hostname command, 227
hostnames
  ping command, 69
  validation, 55
hosts
  nslookup, 70
  operating systems, verification, 307
Hot Standby Router Protocol. See HSRP
HQ Routers
  EIGRP (Enhanced Interior Gateway Protocol)
    configuration, 105
    IPv6 configuration, 133
  Frame Relay configuration, 248
  GRE tunnel configurations, 259
  OSPFv3 (Open Shortest Path First version 3), 178
  point-to-multipoint configuration, 248
  point-to-point Frame Relay, 246
HSRP (Hot Standby Router Protocol), 37-38
  interface tracking, 38
  in IPv6, 40
  load balancing, 39
  in service deployments, 39-40
hub-and-spoke networks
  Frame Relay, 237
  L3VPNs, 370
  WANs (wide-area networks), 188-189
hypervisor, 72-74
IANA (Internet Assigned Numbers Authority), 76
ICMP (Internet Control Messaging Protocol), 51
identification of paths
IPv4 (Internet Protocol version 4), 63-66
IPv6 (Internet Protocol version 6), 81
IDs
areas, 148
routers, 148
tags, 319
IFS (Cisco IOS File System), 302
IGP (Interior Gateway Protocol), 91-93
images, IOS
loading, 297-300
locating to load, 295-297
managing, 305
upgrading, 308-311
implementation
EIGRP (Enhanced Interior Gateway Protocol), 91
IPv6 (Internet Protocol version 6), 124-136
troubleshooting, 115-124
EtherChannel, 31
scalable medium-sized networks, 1
configuring trunks, 7
creating VLANs (virtual LANs), 4-6
DTP (Dynamic Trunking Protocol), 8-9
overview of VLANs (virtual LANs), 2
troubleshooting VLANs (virtual LANs), 9-10
trunk operations, 6-7, 10-11
scalable multiarea networks with OSPF, 143
VPNs (virtual private networks), 185
INCMP (Incomplete) code, 82
incoming filtering, 122
increasing bandwidth with EtherChannel, 29-35
infrastructure
Cisco Prime Infrastructure, 270
MPLS (Multiprotocol Label Switching), 261-264
INIT state, 166
input
errors, 61
queue drops, 60
In-Service Software Upgrade. See ISSU
installing Cisco IOS
evaluation license, 273-322
permanent licenses, 321-322
integrated CSU/DSU
back-to-back routers, 209-216
configuration, 215-216
modules, 214
Integrated Service Router. See ISR
Integrated Services Digital Network. See ISDN
integrity, 256, 271
interconnections, 191. See also connections
interface interface command, 244
interface interface.subinterface point-to-multipoint command, 249
interface interface.subinterface point-to-point command, 246
interface serial interface_number command, 213
interface serial port/mod command, 224, 227
interface tunnel<tunnel_number> command, 259

interfaces
analog phone lines, 201
authentication, configuration, 114
costs, 175
EIA/TIA-232, 195
EIGRP (Enhanced Interior Gateway Protocol)
  enabling, 120
  verification, 134
EtherChannel. See EtherChannel
Ethernet trunks, 6
LMIs (Local Management Interfaces), 236, 249
multilink PPP (Point-to-Point Protocol), 230-232
NetFlow, 287
OSPF (Open Shortest Path First), 148
passive
  EIGRP (Enhanced Interior Gateway Protocol), 108-111
  OSPF (Open Shortest Path First), 170
resets, 61
routers, 291
serial, 209-214
status, 63
tracking, 38
V.35, 195
WICs (WAN interface cards), 196
Interior Gateway Protocol. See IGP
Intermediate System-to-Intermediate System. See IS-IS
internal component review, routers, 289-291

Internet Assigned Numbers Authority (IANA), 76
Internet-based extranets, 210
Internet Control Messaging Protocol. See ICMP
Internet Protocol. See IP
Internet Protocol version 4. See IPv4
Internet Protocol version 6. See IPv6
interpreting Cisco IOS image filenames, 305-306
intervals, 148
inverse ARP (Address Resolution Protocol), 236
IOS
  configuration, 300-302
defects, researching, 343-345
devices, collecting diagnostic information, 340-341
images
  interpreting filenames, 305-306
  loading, 297-300
  locating to load, 295-297
  managing, 305
  upgrading, 308-311
licensing, 315
  backing up, 325
Cisco IOS 15 licensing and packaging, 316
evaluation license installation, 273-322
obtaining, 318-319
overview of, 315
permanent license installation, 321-322
prior to Cisco IOS 15, 316-317
rehosting, 327-328
uninstalling permanent licenses, 325-327
verification, 287-321
loading, 293
password recovery, 313
trap configuration, 273
IP (Internet Protocol)
addresses, DRs/BDRs, 149
packets, debugging, 350
ports to Telnet, 55
routing tables, 67, 290
ip address ip_address subnet_mask command, 244
ip address ip_v4_address subnet_mask command, 224, 227
ip default-network command, 67
ip flow-export destination ip-address udp-port command, 287
ip flow-export version version command, 287
ip flow command, 287
ip host name ip_address command, 69
ip ospf cost cost command, 160
ip ospf process_id area-id area_id command, 170
IPSec (IP Security), 255-256
IPv4 (Internet Protocol version 4)
EIGRP (Enhanced Interior Gateway Protocol), 125
multiarea IPv4 implementation, 154
troubleshooting
ACLs (access control lists), 71-72
CDP (Cisco Discovery Protocol), 58-60
connections, 48
default gateway issues, 66
default gateway issues, 66
default gateway issues, 81-83
end-to-end components, 48-51
identification of paths, 63-66
name resolution issues, 68
physical connection issues, 60-63
verifying connections, 51-58
virtual environments, 72-74
IPv6 (Internet Protocol version 6)
EIGRP (Enhanced Interior Gateway Protocol)
command syntax, 130-131
configuration, 133-135
feasible successors, 128-129
implementation, 124-136
load balancing, 129
theory of operation, 124
troubleshooting, 135
verification, 131-132
HSRP (Hot Standby Router Protocol), 40
troubleshooting, 75
ACLs (access control lists), 84-86
construction of addresses, 75-76
default gateway issues, 81-83
default gateway issues, 81-83
default gateway issues, 81-83
default gateway issues, 81-83
end-to-end connections, 78-80
identification of paths, 81
name resolution issues, 83
neighbor discovery in, 80-82
unicast addresses, 76-77
virtual environments, 86
ipv6 router ospf process-id are area-id command, 179
ipv6 router ospf process-id command, 179
ISDN (Integrated Services Digital Network), 199
IS-IS (Intermediate System-to-Intermediate System), 93
isolation, memory, 330
ISR (Integrated Service Router), 340
ISSU (In-Service Software Upgrade), 330
ITU-T (International Telecommunication Union), 195

K

K values, 127
   EIGRP (Enhanced Interior Gateway Protocol), 103
keys
   chains, 114
   PAK (Product Activation Key), 316-318

L

L3VPN (Layer 3 VPN) configuration, 369-372
LACP (Link Aggregation Control Protocol), 32-33
LANE (LAN Emulation), 198
last-mile links, 207
late collisions, 61
Layer 2
   flow control, 197
   MPLS (Multiprotocol Label Switching), 263
   WANs (wide-area networks), 197-199
Layer 3
   connections, troubleshooting, 63
   MPLS (Multiprotocol Label Switching), 263
   reachability, 168
Layer 3 VPN. See L3VPN
layouts. See formatting
learning, 14
leased dark fiber, 208
leased lines, 212
levels of syslog logging, 279
license boot module command, 323
licensing, Cisco IOS, 315
   backing up, 325
   Cisco IOS 15 licensing and packaging, 316
   evaluation license installation, 273-322
   obtaining, 318-319
   overview of, 315
   permanent license installation, 321-322
   prior to Cisco IOS 15, 316-317
   rehosting, 327-328
   uninstalling permanent licenses, 325-327
   verification, 287-321
linecode code_type command, 217
lines, serial, 63
Link Aggregation Control Protocol. See LACP
link-state acknowledgments. See LSAcks
link-state advertisements. See LSAs
link-state protocols, 94
link-state requests. See LSRs
link-state routing protocols, 144-146, 150
link-state updates. See LSUs
links
circuit-switched communication, 204
dedicated communication, 204
EtherChannel, 31
Ethernet, troubleshooting, 62
last-mile, 207
packet-switched communication, 205
point-to-point, 6
PPP (Point-to-Point Protocol), 221
serial communication, 210
switched communication, 204
WANs (wide-area networks), 203
links-state databases. See LSDBs
Linux, 330
listening, 14
lists
ACLs (access control lists). See ACLs
distribute, filtering, 122
LMIs (Local Management Interfaces), 236, 249
load balancing
EIGRP (Enhanced Interior Gateway Protocol), 99, 103, 110-112, 129
GLBP (Gateway Load-Balancing Protocol), 40-41
HSRP (Hot Standby Router Protocol), 39
loading
Cisco IOS images, 297-300
IOS, 293
state, 166
local access rates, 235
Local Management Interfaces. See LMIs
locations
Cisco IOS images to load, 295-297
VLANs (virtual LANs), 2
logging, syslog. See syslog
lookup, DNS (Domain Name Server), 69
loopback
plugs, T1 lines, 216
unicast addresses, 76
loop-free classless routing, 99
loops
avoidance, 13
bridging, 18, 26
guards, 21
STP (Spanning Tree Protocol), 13
LSAcks (link-state acknowledgments), 150
LSAs (link-state advertisements), 144-145
OSPF (Open Shortest Path First), 153
OSPFv3 (Open Shortest Path First version 3), 177-178
LSDBs (links-state databases), 144-145, 149-150
LSRs (link-state requests), 149
LSUs (link-state updates), 150
M
MAC (Media Access Control)
addresses, 10, 23, 58
Address fields, 23
databases, troubleshooting, 13
management, 269. See also network
device management
Management Information Bases. See
MIBs
managers, SNMP (Simple Network
Management Protocol), 270
MANs (metropolitan-area networks),
207-209
maps
addresses, Frame Relay, 240-243
topologies, 145
masks
networks, 148
subnet
classful routing, 94
VLSMs (variable-length subnet
masks), 99
MEC (MultiChassis EtherChannel),
31
Media Access Control. See MAC
memory
caches, 290
flash, 290, 303
isolation, 330
NVRAM (nonvolatile RAM), 291
RAM (random-access memory), 290
ROM (read-only memory), 290
merging configurations, 312
messages
CDP (Cisco Discovery Protocol), 60
description, 281
dynamic routing, 92
facility, 281
flow, 222
MNEMONIC, 281
seq no, 281
severity, 281
syslog, 279-281
timestamp, 281
metrics
calculations, 128
EIGRP (Enhanced Interior Gateway
Protocol), 103-104, 126
OSPF (Open Shortest Path First),
146-147
viewing, 112
Metro Ethernet, 209
metropolitan-area networks. See
MANs
MIBs (Management Information
Bases), 270
polling data, monitoring, 272
SNMP (Simple Network
Management Protocol), 275-276
mismatch
trunks, 11
VLANs (virtual LANs), 59
MNEMONIC message, 281
modems. See also connections
cable, 194
DSL (digital subscriber line), 193
WANs (wide-area networks), 192
modes
DTP (Dynamic Trunking Protocol), 8
EXEC, 314, 341
LACP (Link Aggregation Control
Protocol), 33
PAgP (Port Aggregation Protocol),
32
read-only, 274
modification
bandwidth references, 147
configuration registers, 294
neighbors, 123
OSPF (Open Shortest Path First) costs, 147

modules
integrated CSU/DSU, 214
protocol-dependent, 99
WAAS (Wide Area Application Services), 300

monitoring
polling data in SNMP, 272
traps in SNMP, 273

Morris, Scott, 72

MPLS (Multiprotocol Label Switching), 199-200, 261-264

multiarea IPv4 implementation
OSPF (Open Shortest Path First), 154
components of troubleshooting, 165-168
configuration, 158-160
neighbors, 168-172
neighbor states, 162-165
NSSAs (not-so-stubby areas), 156
planning implementation, 158
single-area vs., 155
stub areas, 155-156
totally stub areas, 157
troubleshooting, 162
verification, 160-162
OSPFv3 (Open Shortest Path First version 3), 176-180
multicast replication, 238

MultiChassis EtherChannel. See MEC

multilink PPP (Point-to-Point Protocol) over serial line configuration, 228-232
multiple frame transmission, 13
multiple syslog destinations, 282
Multiprotocol Label Switching. See MPLS

N

NADs (network access devices), 195
name resolution
dynamic name resolution, 69-71
IPv4 (Internet Protocol version 4), 68
IPv6 (Internet Protocol version 6), 83
static name resolution, 68-69
NAT (Network Address Translation), 74, 94
navigation, Cisco Feature Navigator, 308
NBMA (nonbroadcast multiaccess) networks, 166, 238
NDP (nondesignated port), 14
negotiation, automatic trunk, 8
neighbors
adjacencies, 147-149
discovery, 99
Frame Relay, 238
in IPv6 (Internet Protocol version 6), 80-82
EIGRP (Enhanced Interior Gateway Protocol), 106, 118-121, 134
link-state routing protocols, 145-146
modification, 123
OSPF (Open Shortest Path First), 168-172
states, multiarea OSPF, 162-165
NetFlow, 283-288
  architecture, 285-286
  configuration, 286-287
  verification, 287-288
netsh interface ipv6 show neighbor
  Windows command, 80
network access devices. See NADs
Network Address Translation. See NAT
network-clock-select priority
  t1_or_e1 slot/port command, 217
network device management, 269
  Cisco IOS-XE, 330
  Cisco IOS-XR, 329-330
  Cisco NX-OS, 331
  configuration, 270
IOS licensing, 315
  backing up, 325
  Cisco IOS 15 licensing and packaging, 316
  evaluation license installation, 322-273
  obtaining, 318-319
  overview of, 315
  permanent license installation, 321-322
  prior to Cisco IOS 15, 316-317
  rehosting, 327-328
  uninstalling permanent licenses, 325-327
  verification, 287-321
routers, 288
  Cisco IOS password recovery, 313
  configuration files, 311-313
  configuration registers, 293-295
IFS (Cisco IOS File System), 302
temporary component review, 289-291
interpreting Cisco IOS image filenames, 305-306
loading Cisco IOS images, 297-300
locating Cisco IOS images to load, 295-297
managing Cisco IOS images, 305
power-up sequences, 292-293
ROM (read-only memory), 291-292
selecting/loading configurations, 300-302
upgrading Cisco IOS images, 308-311
SNMP (Simple Network Management Protocol)
  configuration, 276-279
  message formats (syslog), 281
  MIBs (Management Information Bases), 275-276
NetFlow, 283-288
  obtaining data from agents, 271
  overview of syslog, 279-280
  polling data, monitoring in, 272
  sending data to agents, 274
  syslog configuration, 281
  traps, monitoring in, 273
  versions, 270-271
network interface cards. See NICs
Network Management System. See NMS
network network wildcard_mask area area_id command, 160
networks. See also connections
  automatic summarization, 123
customer, 262
destination, path selection, 146
failures, troubleshooting, 63
interfaces, analog phone lines, 201
ISDN (Integrated Services Digital Network), 199
MANs (metropolitan-area networks), 207-209
masks, 148
MPLS (Multiprotocol Label Switching), 261-264
NBMA (nonbroadcast multiaccess), 166
provider, 241
PVST+ (Per-VLAN Spanning Tree Plus), 21-23
scalable medium-sized. See scalable medium-sized networks
SONET (Synchronous Optical Network), 198
two-router IPv6, 133
VPNs (virtual private networks). See VPNs
WANs (wide-area networks), 185-186. See also WANs
wireless, 194, 199
Nexus Operating System. See NX-OS
NICs (network interface cards), 6
NMS (Network Management System), 270
  configuration, 272
  traps, monitoring, 273
no debug command, 350
no shutdown command, 213, 224
nonbackbone areas, 151
nonbroadcast multiaccess. See NBMA
non-Cisco equipment, running CDP on, 58
nondesignated port. See NDP
nonvolatile RAM. See NVRAM
normal areas, 151
notation, CIDR (classless interdomain routing), 76
not-so-stubby areas. See NSSAs
nslookup
  IPv4 (Internet Protocol version 4), 70
  IPv6 (Internet Protocol version 6), 84
NSSAs (not-so-stubby areas), 156
numbers, AS (autonomous systems), 119
NVRAM (nonvolatile RAM), 291-293
NX-OS (Nexus Operating System), 340

O

Object IDs. See OIDs
obtaining IOS licensing, 318-319
OIDs (Object IDs), 275
one-line summary per channel group, 35
Open Shortest Path First. See OSPF
operating expense. See OPEX
operating systems
  Cisco NX-OS, 331
  host verification, 307
  RAM (random-access memory), 290
operations
  protocols, verification, 359-361
  trunks, 6-7
OPEX (operating expense), 193
optical fiber converters, 194
optimizing redundancy, 29-35
options
  OSPF (Open Shortest Path First), 149
  WANs (wide-area networks)
    links, 203
    private connection, 204-205
    public connection, 205-207
OSPF (Open Shortest Path First), 93
  areas
    structures, 150
    types, 150-153
AS (autonomous systems), 151
costs, modification, 147
link-state routing protocols, 144-146
LSAs (link-state advertisements), 153
LSDBs (links-state databases), building, 149-150
metrics, 146-147
multiarea IPv4 implementation, 154
  components of troubleshooting, 165-168
  configuration, 158-160
  neighbor states, 162-165
  NSSAs (not-so-stubby areas), 156
  planning implementation, 158
  single-area vs., 155
  stub areas, 155-156
  totally stub areas, 157
  troubleshooting, 162
  verification, 160-162
neighbors
  adjacencies, 147-149
  troubleshooting, 168-172
overview of, 144
path selection, troubleshooting, 174-176
routing tables, troubleshooting, 172-174
scalable multiarea networks, implementation, 143
OSPFv3 (Open Shortest Path First version 3), 176-180
output
  characters, ping command, 54
debugging
    capturing, 345-350
    limiting, 351
queue drops, 61
Output Interpreter, applying, 341

P

P (Provider) routers, 262
packaging
  Cisco IOS 15 licensing and, 316
    prior to Cisco IOS 15, 316-317
packet-switched communication links, 205
packets
  buffers, 290
  DBDs (database descriptors), 149
  IP (Internet Protocol), debugging, 350
  LSACKs (link-state acknowledgments), 150
LSDBs (links-state databases), updating, 149
LSRs (link-state requests), 149
LSUs (link-state updates), 150
metrics. See metrics
NetFlow, 284
types, EIGRP, 100-101
PAGP (Port Aggregation Protocol), 31-32
PAK (Product Activation Key), 316, 318
PAP (Password Authentication Protocol), 198, 222
partial-mesh networks
  Frame Relay, 236
  WANs (wide-area networks), 189
passive-interface interface command, 171
passive interfaces
  EIGRP (Enhanced Interior Gateway Protocol), 108-111
  OSPF (Open Shortest Path First), 170
Password Authentication Protocol. See PAP
password recovery, IOS, 313
paths
  identification of
    IPv4 (Internet Protocol version 4), 63-66
    IPv6 (Internet Protocol version 6), 81
selection
  destination networks, 146
  EIGRP (Enhanced Interior Gateway Protocol), 101, 126
OSPF (Open Shortest Path First), troubleshooting, 174-176
PCMCIA (Personal Computer Memory Card International Association), 291
percent sign (%), 83
permanent IOS license installation, 321-322
permanent virtual circuits. See PVCs
PE (Provider Edge) routers, 262
Personal Computer Memory Card International Association. See PCMCIA
Per-VLAN Spanning Tree Plus. See PVST+
physical connection issues, troubleshooting, 60-63
physical interfaces. See interfaces
physical locations, VLANs (virtual LANs), 2
PIDs (product IDs), 319
ping command, 51
  ACLs (access control lists)
    triggering debugging, 355
    troubleshooting, 72
  EIGRP (Enhanced Interior Gateway Protocol), troubleshooting, 118
    extended, 53
    IPv6 (Internet Protocol version 6), 79
    output characters, 54
    static name resolution, 69
placement of routers, troubleshooting, 87
plain old telephone system (POTS), 194
planning OSPF multiarea IPv4 implementations, 158
platform abstraction, 330
plugs, loopback, 216
point-to-multipoint configuration, 247-249
point-to-point links, 6
point-to-point networks, WANs, 191
Point-to-Point Protocol. See PPP
point-to-point subinterface configuration, 245-246
polling data, monitoring in SNMP, 272
populating routing tables, 64
Port Aggregation Protocol. See PAgP
Portfast, 20, 28
ports
channels, viewing, 35
disabled, 14
EtherChannel, 34
IP (Internet Protocol), Telnet to, 55
MAC (Media Access Control) address tables, 58
POST (power-on self-test), 292
POTS (plain old telephone system), 194
power-on self-test. See POST
power-up sequences, routers, 292-293, 302
PPP (Point-to-Point Protocol), 198
configuration, 223-227
WANs (wide-area networks), 220-221
ppp authentication chap command, 227
prevention, bridging loops, 18
priority routers, 149
private connection options, WANs, 204-205
private dark fiber, 208
private (link-local) unicast addresses, 76
privileged EXEC mode, 314
PROBE code, 82
processes, dynamic routing, 92
Product Activation Key. See PAK
protocol-dependent modules, 99
protocols
ARP (Address Resolution Protocol), 51, 57, 236
BGP (Border Gateway Protocol), 93, 128
CDP (Cisco Discovery Protocol), 13, 58-60
CHAP (Challenge-Handshake Authentication Protocol), 198, 359
distance vector, 93
DTP (Dynamic Trunking Protocol), 8-9
EIGRP (Enhanced Interior Gateway Protocol). See EIGRP
EtherChannel, 31
exchange, 164
FTP (File Transfer Protocol), 303
GLBP (Gateway Load-Balancing Protocol), 40-41
HDLC (High-Level Data Link Control), 197
Hello, 163
HSRP (Hot Standby Router Protocol), 37-38
interface tracking, 38
in IPv6, 40
load balancing, 39
  in service deployments, 39-40
IGP (Interior Gateway Protocol), 91, 93
LACP (Link Aggregation Control Protocol), 32-33
link-state, 94
operations, verification, 359-361
PAGP (Port Aggregation Protocol), 31-32
PAP (Password Authentication Protocol), 198
PPP (Point-to-Point Protocol), 198
RIP (Routing Information Protocol), 93
routings, 92
  administrative distances, 95-98
  classification of, 93
Frame Relay, 237-239
hierarchies, link-state, 150
link-state, 144-146
OSPF (Open Shortest Path First). See OSPF
RTP (Reliable Transport Protocol), 99
SDLC (Synchronous Data Link Control), 197
SFTP (Secure File Transfer Protocol), 274
SNMP (Simple Network Management Protocol), 270
STP (Spanning Tree Protocol), 12
  analysis, 24-26
  failures, 26-28
  types, 20-21
WANs (wide-area networks)
  CHAP (Challenge-Handshake Authentication Protocol), 222-223
  HDLC (High-Level Data Link Control), 218-220
  Layer 2, 197-199
  PAP (Password Authentication Protocol), 222
  PPP (Point-to-Point Protocol), 220-221
Provider. See P
Provider Edge. See PE
provider networks, 241
Pseudowire, 369
public connection options, WANs, 205-207
PVCs (permanent virtual circuits), 235, 251
PVST+ (Per-VLAN Spanning Tree Plus), 20-23

Q
QoS (quality of service), 61
  WANs (wide-area networks), 200
queries, nslookup, 70
queues, drops, 60

R
RAM (random-access memory), 290
rapid convergence, 99
Rapid STP. See RSTP
RCP (Remote Copy Protocol), 303
RCS (Real Time Control System), 191
reachability, 92
   Frame Relay, 237-239
   Layer 3, 168
   OSPF (Open Shortest Path First), 168
   REACH (Reachable) code, 82
read-only memory. See ROM
read-only mode, SNMP, 274
Real Time Control System. See RCS
recovery
   neighbor discovery, 99
   passwords, IOS, 313
re-distribute command, 153
reduced bandwidth usage, 99
redundancy
   bandwidth, increasing with
      EtherChannel, 29-35
   Cisco IOS-XR, 330
   default gateways, 36-41
topologies
   overview of, 12-15
   switches, 11
   WANs (wide-area networks), 191
references, bandwidth
   modification, 147
   verification, 176
Regional Internet Registries (RIR), 76
registers, configuration, 291-295
registration, Cisco Licenses
   Registration Portal, 318
rehosting IOS licenses, 327-328
relationships, neighbors, 168
reliability, EIGRP, 103
Reliable Transport Protocol. See RTP
reload command, 320
remote-access VPNs, 253
Remote Copy Protocol. See RCP
remote sites, interconnections, 191
repositories, files, 304
Request for Comments. See RFCs
researching Cisco IOS software defects, 343-345
reserved unicast addresses, 76
resets, interfaces, 61
resiliency, 331
restarting routers, 321
results, applying Output Interpreter, 341
reviewing
   ACL (access control list) counters, 355
   EIGRP (Enhanced Interior Gateway Protocol) neighbors, 134
   licenses, 318
   STP (Spanning Tree Protocol), 24-26
RFCs (Request for Comments), 91
RIP (Routing Information Protocol), 93
RIR (Regional Internet Registries), 76
RJ-45 straight-through cable, 196
ROM (read-only memory), 290-292
ROMmon (ROM monitor), 292, 313
Root Guard, 21, 28
root port. See RP
router-id router_id command, 179
router ospf process_id command, 160
routers
   ABRs (Area Boundary Routers), 152
   active, 37
ARP (Address Resolution Protocol) caches, 57
ASBRs (Autonomous System Boundary Routers), 152-153
autoconfiguration, 301
backbone configuration, 151
back-to-back, integrated CSU/DSU, 209-216
Branch Routers
  EIGRP configuration, 105
  EIGRP IPv6 configuration, 133
  Frame Relay configuration, 248
  GRE tunnel configurations, 259
  OSPFv3 (Open Shortest Path First version 3), 178
  point-to-multipoint configuration, 248
  point-to-point Frame Relay, 246
  SNMP configuration, 278
CDP (Cisco Discovery Protocol), 58
CE (Customer Edge), 262
HQ Routers
  EIGRP configuration, 105
  EIGRP IPv6 configuration, 133
  Frame Relay configuration, 248
  GRE tunnel configurations, 259
  OSPFv3 (Open Shortest Path First version 3), 178
  point-to-multipoint configuration, 248
  point-to-point Frame Relay, 246
IDs, 148
interfaces, 291
ISR (Integrated Service Router), 340
neighbor OSPF, 147
network device management, 288
  Cisco IOS password recovery, 313
  configuration files, 311-313
  configuration registers, 293-295
  IFS (Cisco IOS File System), 302
  internal component review, 289-291
  interpreting Cisco IOS image filenames, 305-306
  loading Cisco IOS images, 297-300
  locating Cisco IOS images to load, 295-297
  managing Cisco IOS images, 305
  power-up sequences, 292-293
  ROM (read-only memory), 291-292
  selecting/loading configurations, 300-302
  upgrading Cisco IOS images, 308-311
normal area configuration, 151
P (Provider), 262
PE (Provider Edge), 262
placement, troubleshooting, 87
priority, 149
restarting, 321
sources, determination of, 172
standby, 37
troubleshooting, 340
  applying Output Interpreter, 341
collecting IOS device information, 340-341
researching Cisco IOS software defects, 343-345
types, 150-153
virtual, redundancy, 36
WANs (wide-area networks), 192

routes
feasible successor, 103
filtering, troubleshooting EIGRP, 122-124
path selection, 101
unadvertised, troubleshooting EIGRP, 121

routing
classful, 94-95
classless, 94-95
CRS (Carrier Routing System), 291
domains, 92
dynamic, overview of, 92-106
entries, troubleshooting inaccurate, 124
GRE (Generic Routing Encapsulation), 256-261
protocols, 92
administrative distances, 95-98
classification of, 93
Frame Relay, 237-239
hierarchies, link-state, 150
link-state, 144-146
OSPF (Open Shortest Path First). See OSPF
tables, 92
IP (Internet Protocol), 67
OSPF (Open Shortest Path First), 172-174

reviewing using passive interfaces, 109
Unicast, 64
updating, 95, 108
Routing Information Protocol. See RIP
RP (root port), 14, 17
RSTP (Rapid STP), 20
RTP (Reliable Transport Protocol), 99
rules, ACLs (access control lists), 85
running
configuration files, RAM, 290
traceroute, 52
runts, 61

S
scalable medium-sized networks
DTP (Dynamic Trunking Protocol), 8-9
implementing, 1
trunks
configuring, 7
operations, 6-7
troubleshooting, 10-11
VLANs (virtual LANs)
creating, 4-6
overview of, 2
troubleshooting, 9-10
scalable multiarea networks, OSPF implementation, 143
scaling delay, 127
SDLC (Synchronous Data Link Control) protocol, 197
searching Cisco IOS images to load, 295-297
Secure File Transfer Protocol. See SFTP

Securing the Data Plane
Configuration Guide Library, Cisco IOS Release 15M&T, 72

security
IPSec (IP Security), 255-256
SNMP (Simple Network Management Protocol), 271
VPNs (virtual private networks), 185

selection
Cisco IOS configurations, 300-302
DP (designated port), 19
paths, 101, 146. See also paths, selection

sending data to SNMP agents, 274
seq no message, 281
serial cabling, WANs, 195
serial communication links, 210
serial encapsulation, WANs, 232
serial interfaces, WANs, 209-214
serial lines, 63
encapsulation, 219
multilink PPP (Point-to-Point Protocol) configuration, 228-232

serial numbers. See SNs

servers
SFTP (Secure File Transfer Protocol), 274
Telnet, 55

service provider demarcation points, WANs, 200

services
HSRP (Hot Standby Router Protocol), 39-40
ISDN (Integrated Services Digital Network), 199

WAAS (Wide Area Application Services), 300
WANs (wide-area networks), 187

SET command, 274
settings. See configuration
severity message, 281
SFTP (Secure File Transfer Protocol), 274
sharing traffic, EIGRP, 113-114

shortest path first. See SPF

show commands
show access-lists command, 71
show buffers command, 340
show cdp neighbors command, 59
show controllers command, 340
show debug command, 350
show etherchannel port-channel command, 35
show etherchannel summary command, 34
show flash0: command, 306
show glbp command, 41
show interface command, 60, 104, 340
show interface interface switchport command, 10
show interface port-channel command, 34
show interfaces command, 7, 62, 249
show ip cache flow command, 288
show ip eigrp neighbors command, 106-107
show ip eigrp topology command, 110-111
show ip flow interface command, 287
show commands

show ip interface brief command, 260
show ip interface command, 168, 260
show ip ospf interface command, 170, 175
show ip ospf neighbor command, 172
show ip protocols command, 120, 170
show ip route command, 63-65, 108-109, 173
show ipv6 eigrp neighbors command, 134
show license command, 320, 340
show license udi command, 319
show mac address-table command, 58
show process cpu command, 340
show processes memory command, 340
show running-config command, 302, 340
show snmp additional_options command, 278
show spanning-tree command, 25
show stacks command, 340
show startup-config command, 302
show tech command, 341
show version command, 298, 321, 340
show vlan command, 5
shutdown command, 227
signaling, Frame Relay, 239-240
SIMMs (single in-line memory modules), 291

Simple Network Management Protocol. See SNMP
single-area OSPF, 155
single in-line memory modules. See SIMMs
site-to-site VPNs, 253
SNMP (Simple Network Management Protocol), 270
network device management
configuration, 276-279
message formats (syslog), 281
MIBs (Management Information Bases), 275-276
NetFlow, 283-288
obtaining data from agents, 271
overview of syslog, 279-280
polling data, monitoring in, 272
sending data to agents, 274
syslog configuration, 281
traps, monitoring in, 273
versions, 270-271
snmp-server chassis-id serial_no command, 278
snmp-server community string [RO | RQ] command, 278
snmp-server contact contact_name command, 278
snmp-server host ip_address trap community_string command, 278
snmp-server location location command, 278
SNs (serial numbers), 319
software. See also applications
Cisco IOS. See IOS
defects, researching, 343-345
licenses. See licensing
VPNs (virtual private networks), 205
SONET (Synchronous Optical Network), 198
sources, determination of routers, 172
Spanning Tree Protocol. See STP
SPF (shortest path first), 94, 145
split horizons, 238
spoke networks, 188. See also hub-and-spoke networks
STALE code, 82
standby
groups, 37
routers, 37
state, 13
starting routers, 292-293, 302
states
HSRP (Hot Standby Router Protocol), 38
multiarea OSPF neighbors, 162-165
static name resolution, 68-69
statistics, NetFlow, 288
status
interfaces, 63
NetFlow, 288
protocols, verification of EIGRP neighbors, 118
STP (Spanning Tree Protocol), 12
analysis, 24-26
failures, 26-28
types, 20-21
structures, OSPF areas, 150
stub areas, 155-156
subinterfaces
NBMA (nonbroadcast multiaccess) networks, 238
point-to-point configuration, 245-246
subnet masks
classful routing, 94
VLSMs (variable-length subnet masks), 99
summarization, automatic network, 123
SVCs (switched virtual circuits), 235
switched communication links, 204
switched virtual circuits. See SVCs
switches
CDP (Cisco Discovery Protocol), 58
default configuration, 4
MPLS (Multiprotocol Label Switching), 200, 261-264
redundancy, 11-15
WANs (wide-area networks), 185, 192
switchport access vlan command, 5
switchport nonegotiate interface command, 9
switch-to-switch connectivity, 6
Synchronous Data Link Control protocol. See SDLC protocol
Synchronous Optical Network. See SONET
syslog
configuration, 281
messages, formatting, 281
overview, 279-280
T1 lines
crossover cables, 209
integrated CSU/DSU, 215
loopback plugs, 216
WANs (wide-area networks), 200-201

Tables
MAC (Media Access Control) addresses, 10, 58
routed, 92
IP (Internet Protocol), 67
OSPF (Open Shortest Path First), 172-174
reviewing using passive interfaces, 109
Unicast, 64

TAC (Technical Assistance), 339, 345
tags, ID, 319
Technical Assistance. See TAC
Telnet, 55
to IP ports, 55
IPv6 (Internet Protocol version 6) connections, 67
terminal-emulation program, 346
terminal monitor command, 346
termination
  cable modems, 202
  DSL (digital subscriber line), 201
  WANs (wide-area networks), 203
testing basic connectivity, 51
timestamp message, 281
Time to Live. See TTL

Tools
Bug Toolkit, 344
nslookup
  IPv4 (Internet Protocol version 4), 70
  IPv6 (Internet Protocol version 6), 84
ping command, 51-53
traceroute, 51
  IPv6 (Internet Protocol version 6), 79
  running, 52

Topologies
  EtherChannel, 29-35
IPv6 (Internet Protocol version 6), 135
  maps, 145
redundancy
  overview of, 12-15
  switches, 11
STP (Spanning Tree Protocol), 15
WANs (wide-area networks)
  Frame Relay, 236-237
  full-mesh networks, 189-191
  hub-and-spoke networks, 188-189
  partial-mesh networks, 189
  point-to-point networks, 191
totally stub areas, 157
traceroute, 51
  IPv6 (Internet Protocol version 6), 79
  running, 52
tracert command, 52
tracking interfaces, 38
traffic sharing, EIGRP, 113-114
transitions
carrier, 61
from exstart to full state, 162
transmissions, aborted, 62
traps, monitoring SNMP, 273
triggering debugging
ACLs (access control lists), 351-356
conditionally, 356-357
troubleshooting, 339
ACLs (access control lists), 71-72
cables, 50
connections, 47
data centers, 86
default gateways, 66
devices, debugging, 345, 357-359
DNS (Domain Name Server), 50
EIGRP (Enhanced Interior Gateway Protocol), 115-124
  automatic network summarization, 123
  components, 115-118
IPv6 (Internet Protocol version 6), 135
  neighbors, 118-121
  route filtering, 122-124
  routing tables, 121
  unadvertised routes, 121
Ethernet links, 62
IPv4 (Internet Protocol version 4), 48
  ACLs (access control lists), 71-72
  CDP (Cisco Discovery Protocol), 58-60
  default gateway issues, 66
  end-to-end components, 48-51
identification of paths, 63-66
name resolution issues, 68
physical connection issues, 60-63
verifying connections, 51-58
virtual environments, 72-74
IPv6 (Internet Protocol version 6), 75
  ACLs (access control lists), 84-86
  construction of addresses, 75-76
  default gateway issues, 81-83
  end-to-end connections, 78-80
  identification of paths, 81
  name resolution issues, 83
  neighbor discovery in, 80-82
  unicast addresses, 76-77
  virtual environments, 86
Layer 3 connections, 63
MPLS (Multiprotocol Label Switching),
name resolution issues
  dynamic name resolution, 69-71
  static name resolution, 68-69
NBMA (nonbroadcast multiaccess) networks, 238
OSPF (Open Shortest Path First)
  components, 165-168
  multiarea IPv4 implementation, 162
  neighbors, 168-172
  path selection, 174-176
  routing tables, 172-174
overview of, 86
routers, 340

*applying Output Interpreter, 341*

collecting IOS device information, 340-341

placement, 87

researching Cisco IOS software defects, 343-345

STP (Spanning Tree Protocol), 24-26

trunks, 10-11

virtual environments, 72-74

VLANs (virtual LANs), 9-10

VPNs (virtual private networks), 74

WANs (wide-area networks)

Frame Relay, 237-239

serial encapsulation, 232

trunks, 1

configuration, 7

operations, 6-7

troubleshooting, 10-11

TTL (Time to Live), 13

tunnel destination ip_address command, 259

tunnel mode gre ip command, 259

tunnel source ip_address command, 259

tunnels, GRE (Generic Routing Encapsulation), 256-261

two-router IPv6 networks, 133

two-way state, 166

types

OSPF (Open Shortest Path First)

areas, 150-153

of packets, 100-101

of routers, 150-155

STP (Spanning Tree Protocol), 20-21

of unicast addresses, 76

of VPNs (virtual private networks), 253

U

UDIs (universal device identifiers), 319

unadvertised routes, troubleshooting EIGRP, 121

undebug command, 350

unicast addresses, troubleshooting, 76-77

Unicast routing tables, 64

uninstalling permanent licenses, 325-327

universal device identifiers. See UDIs

unspecified unicast addresses, 76

updating

packets, LSDBs, 149

passive interfaces, 108

routing, 95

upgrading

Cisco IOS images, 308-311

ISSU (In-Service Software Upgrade), 330

UplinkFast, 20

username username password password command, 227

user-reported errors, 49

utilities. See tools

V

V.35 interfaces, 195

validation

ACLs (access control lists), 353

hostnames, 55
L3VPN (Layer 3 VPN), 370-372
serial line encapsulation, 219

values
configuration register, 294-295
K, 103, 127

variable-length subnet masks. See VLSMs

variance, EIGRP (Enhanced Interior Gateway Protocol), 112-113

VCs (virtual circuits), 235

verification
advertisements, 172
bandwidth references, 176
CHAP (Challenge-Handshake Authentication Protocol) configuration, 227
devices, debugging, 350-351
EIGRP (Enhanced Interior Gateway Protocol)
configuration, 106-108
IPv6 (Internet Protocol version 6), 131-132
AS numbers, 119

EtherChannel, 34-35
GRE (Generic Routing Encapsulation) tunnels, 260
host operating systems, 307

IOS licensing, 287-321
IPv4 (Internet Protocol version 4) connections, 51-58
IPv6 (Internet Protocol version 6) addresses, 80
connections, 79-80
L3VPN (Layer 3 VPN), 369
NetFlow, 287-288

OSPF (Open Shortest Path First)
multiarea IPv4 implementation, 160-162
OSPFv3 (Open Shortest Path First version 3), 179-180
protocol operations, 359-361
SNMP (Simple Network Management Protocol), 276-279
VLANs (virtual LANs), configuration, 4-6
WANs (wide-area networks), Frame Relay, 249-252

versions of SNMP (Simple Network Management Protocol), 270-271

video collaboration, 191

viewing
ARP (Address Resolution Protocol) caches, 57
metrics, 112
port channels, 35
routing tables, 67
UDIs (universal device identifiers), 319
VLANs (virtual LANs), 5

virtual circuits. See VCs

virtual environments
IPv4 (Internet Protocol version 4), 72-74
IPv6 (Internet Protocol version 6), 86

virtual LANs. See VLANs

Virtual Private LAN Services. See VPLS

virtual routers, redundancy, 36
virtualization, Cisco NX-OS, 331

vlan global configuration command, 4

vlan vlan_id command, 10
VLANs (virtual LANs)
configuration, 3
creating, 4-6
mismatch, 59
overview of, 2
troubleshooting, 9-10
VLSMs (variable-length subnet masks), 99
voice collaboration, 191
VoIP (Voice over IP) devices, 58
VPLS (Virtual Private LAN Services), 369
VPNs (virtual private networks), 74
clientless, 206
implementation, 185
software, 205
WANs (wide-area networks)
GRE (Generic Routing Encapsulation) tunnels, 256-261
IPSec (IP Security), 255-256
MPLS (Multiprotocol Label Switching), 261-264
overview of, 252-255

W
WAAS (Wide Area Application Services), 300
WAN interface cards. See WICs
WANs (wide-area networks), 185-186
architecture, 188
CHAP (Challenge-Handshake Authentication Protocol), 222-223
core routers, 193
customer logical, 263
devices, 192-195
extranets, 209
Frame Relay, 233
configuration, 243-244
mapping addresses, 240-243
multipoint/point-to-point, 244
overview of, 233-236
point-to-multipoint configuration, 247-249
point-to-point subinterface configuration, 245-246
signaling, 239-240
topologies, 236-237
troubleshooting, 237-239
verifying configuration, 249-252
full-mesh networks, 189-191
HDLC (High-Level Data Link Control) protocol, 218-220
hub-and-spoke networks, 188-189
integrated CSU/DSU
back-to-back routers, 216-209
configuration, 215-216
modules, 214
ISDN (Integrated Services Digital Network), 199
Layer 2 protocols, 197-199
MANs (metropolitan-area networks), 207-209
MPLS (Multiprotocol Label Switching), 200
options
link, 203
private connection, 204-205
overview of, 186-188
PAP (Password Authentication Protocol), 222
partial-mesh networks, 189
point-to-point networks, 191
PPP (Point-to-Point Protocol), 220-221
  configuration, 223-227
  multilink over serial line configuration, 228-232
public connection options, 205-207
routers, 192
serial cabling, 195
serial encapsulation, troubleshooting, 232
serial interface configuration, 209-214
service provider demarcation points, 200
switches, 192
T1 line loopback plugs, 216
T1/E1, 200-201
 termination
  cable modem, 202
  DSL (digital subscriber line), 201
  Ethernet, 203
VPNs (virtual private networks)
  GRE (Generic Routing Encapsulation) tunnels, 256-261
  IPSec (IP Security), 255-256
  MPLS (Multiprotocol Label Switching), 261-264
  overview of, 252-255
X.25, 199
WICs (WAN interface cards), 196
Wide Area Application Services. See WAAS

wide-area networks. See WANs
wireless access points, CDP, 58
wireless networks, 194, 199
  MANs (metropolitan-area networks), 209

X-Z

X.25, 199
zeros, IPv6 (Internet Protocol version 6) addresses, 75