Routing Protocols and Concepts

CCNA Exploration Companion Guide

Rick Graziani • Allan Johnson

Cisco Networking Academy
Mind Wide Open
Routing Protocols and Concepts, CCNA Exploration Companion Guide

Rick Graziani, Allan Johnson

Copyright © 2008 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

Nineth Printing February 2011

Library of Congress Cataloging-in-Publication Data
Graziani, Rick.
Routing protocols and concepts : CCNA exploration companion guide/Rick Graziani, Allan Johnson.
p. cm.
TK5105.543.G73 2007
004.6—dc22
2007042619


This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.
Warning and Disclaimer

This book is designed to provide information about routing protocols and concepts of the Cisco Network Academy CCNA Exploration curriculum. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corporalsales@pearsontechgroup.com

For sales outside the United States please contact: International Sales international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.
About the Authors

Rick Graziani teaches computer science and computer networking courses at Cabrillo College in Aptos, California. Rick has worked and taught in the computer networking and information technology field for almost 30 years. Prior to teaching, Rick worked in IT for various companies including Santa Cruz Operation, Tandem Computers, and Lockheed Missiles and Space Corporation. He holds an M.A. in computer science and systems theory from California State University Monterey Bay. Rick also does consulting work for Cisco and other companies. When Rick is not working, he is most likely surfing. Rick is an avid surfer who enjoys longboarding at his favorite Santa Cruz surf breaks.

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an M.B.A. and an M.Ed. in occupational training and development. He is an information technology instructor at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for the Academy in Learning Systems Development.
About the Technical Reviewers

Nolan Fretz is a college professor in network and telecommunications engineering technology at Okanagan College in Kelowna, British Columbia. He has almost 20 years of experience in implementing and maintaining IP networks and has been sharing his experiences by educating students in computer networking for the past nine years. He holds a master’s degree in information technology.

Charles Hannon is an assistant professor of network design and administration at Southwestern Illinois College. He has been a Cisco Certified Academy instructor since 1998. Charles has a master of arts in education from Maryville University, St. Louis, Missouri, currently holds a valid CCNA certification, and has eight years’ experience in management of information systems. Charles’ priority is to empower students to become successful and compassionate lifelong learners.

Matt Swinford, associate professor of network design and administration at Southwestern Illinois College, has been an active Cisco Certified Academy instructor since 1999. Matt is dedicated to fostering a learning environment that produces certified students and quality IT professionals. Matt has a master of business administration from Southern Illinois University at Edwardsville in Edwardsville, Illinois, and currently holds CCNP, A+, and Microsoft certifications.
Acknowledgments

From Rick Graziani:

First of all, I want to thank my good friend Allan Johnson for the pleasure of writing this book with him. I can’t imagine a better team of two writers contributing to a book that worked so well together to the benefit of its readers. Allan’s unique combination of technical knowledge, writing skills, and graphic skills, along with his commitment to quality, is evident throughout the curriculum and this book.

Cindy Ciriello was a critical member of the development team as an instructional designer, and her assistance and perspective were invaluable to the project. Thank you, Cindy, for all of your help.

The more you know about computer networking, the more you realize what you don’t know. Over the years, friends and network engineers Mark Boolootian and Jim Warner, at the University of California Santa Cruz, and Dave Barnett, Santa Cruz County Office of Education, have been vital resources for me. Our late-night discussions at various restaurants, writing topologies and protocols out on napkins, and discussing a variety of scenarios and issues have been invaluable to me over our many years of friendship. It is always a classic case of four geeks talking nerd-stuff.

Thank you to Fred Baker, Cisco Fellow and former IETF chair, for his support and encouragement over the years. I greatly appreciate his time and the insight he has always graciously provided.

A special thank you to Alex Zinin, author of the book Cisco IP Routing. His book and generous correspondence has detailed routing protocol processes and algorithms for me that I could find nowhere else. His impact and influence can be found throughout this book. Thanks again, Alex!

Special thanks to Mary Beth Ray for her patience and understanding throughout this long process. Mary Beth always provided that voice of calm assurance and guidance whenever needed.

Thank you Dayna Isley and Chris Cleveland for your help in the editing and production stages. I am amazed at the level of cooperation and teamwork required to produce a technical book, and I am grateful for all of your help.

Thanks to all of the technical editors for providing feedback and suggestions. I will take full responsibility for any remaining technical errors in the book.

Special thanks to Pat Farley, who made sure that I continued to get my surf time in every week during this project and therefore maintained my sanity. For those of you who surf, you know how important this is. Thank you, Pat, for your friendship and support.

Finally, I want to thank all of my students over the years. For some reason, I always get the best students. You make my job fun and the reason why I love teaching.
From Allan Johnson:

Thank you, Rick Graziani, for graciously sharing the work of this project with me. It has truly been an honor to serve our students together. Rick has been my teacher for many years. Now I am proud to call him my friend. Fellow students and readers, you might not realize just how dedicated Rick is to “getting it right.” During development, when I would ask him a really tough technical question, his answer many times was, “Let me go look at the algorithm, and I’ll get back to you.”

Cindy Ciriello rounded out the talents of our development effort, insisting on improving the way we present very technical material. As “Agent 99,” you were able to “geek out” with the best of us and helped maintain my sanity during some very crazy days.

Mary Beth Ray, executive editor, you amaze me with your ability to juggle multiple projects at once, steering each from beginning to end. I can always count on you to make the tough decisions.

Thank you to all my students—past and present—who have helped me over the years to become a better teacher. There is no better way to test the effectiveness of a teaching strategy than to present it to a team of dedicated students. They excel at finding the obscurest of errors! I could have never done this without all of your support.
Dedications

For my wife, Teri. Without her patience and understanding, I would not have been able to participate in this project. Thank you for your love and support throughout the countless hours it took me to complete this book and for your understanding that I still needed time to surf.

—Rick Graziani

For my wife, Becky. Without the sacrifices you made during the project, this work would not have come to fruition. Thank you for providing me the comfort and resting place only you can give.

—Allan Johnson
Contents at a Glance

Introduction xxviii

Chapter 1 Introduction to Routing and Packet Forwarding 1

Chapter 2 Static Routing 65

Chapter 3 Introduction to Dynamic Routing Protocols 147

Chapter 4 Distance Vector Routing Protocols 181

Chapter 5 RIP Version 1 219

Chapter 6 VLSM and CIDR 263

Chapter 7 RIPv2 289

Chapter 8 The Routing Table: A Closer Look 337

Chapter 9 EIGRP 391

Chapter 10 Link-State Routing Protocols 469

Chapter 11 OSPF 499

Appendix Check Your Understanding and Challenge Questions Answer Key 561

Glossary of Key Terms 587

Index 599
Contents

Introduction xxviii

Chapter 1 Introduction to Routing and Packet Forwarding 1

Objectives 1

Key Terms 1

Inside the Router 3

Routers Are Computers 4

Routers Are at the Network Center 4

Routers Determine the Best Path 5

Router CPU and Memory 7

CPU 9

RAM 9

ROM 9

Flash Memory 10

NVRAM 10

Internetwork Operating System (IOS) 10

Router Bootup Process 11

Bootup Process 11

Command-Line Interface 14

Verifying Router Bootup Process 14

IOS Version 16

ROM Bootstrap Program 16

Location of IOS 16

CPU and Amount of RAM 16

Interfaces 16

Amount of NVRAM 17

Amount of Flash 17

Configuration Register 17

Router Ports and Interfaces 17

Management Ports 18

Router Interfaces 18

Interfaces Belong to Different Networks 20

Example of Router Interfaces 20

Routers and the Network Layer 21

Routing Is Forwarding Packets 21

Routers Operate at Layers 1, 2, and 3 22

CLI Configuration and Addressing 24

Implementing Basic Addressing Schemes 24

Populating an Address Table 24
Chapter 2  Static Routing 65

Objectives  65

Key Terms  65

Routers and the Network  66
  Role of the Router  66
  Introducing the Topology  67
  Examining the Connections of the Router  68
    Router Connections  68
    Serial Connectors  68
    Ethernet Connectors  70

Router Configuration Review  71
  Examining Router Interfaces  72
    Interfaces and Their Statuses  72
    Additional Commands for Examining Interface Status  74
  Configuring an Ethernet Interface  76
    Configuring an Ethernet Interface  76
    Unsolicited Messages from IOS  77
    Reading the Routing Table  78
    Routers Usually Store Network Addresses  79
  Verifying Ethernet Addresses  80
    Commands to Verify Interface Configuration  80
    Ethernet Interfaces Participate in ARP  81
  Configuring a Serial Interface  82
  Examining Serial Interfaces  83
    Physically Connecting a WAN Interface  83
    Configuring Serial Links in a Lab Environment  84
    Verifying the Serial Interface Configuration  85

Exploring Directly Connected Networks  87
  Verifying Changes to the Routing Table  87
    Routing Table Concepts  88
    Observing Routes as They Are Added to the Routing Table  89
    Changing an IP Address  91
  Devices on Directly Connected Networks  93
    Accessing Devices on Directly Connected Networks  93
    Pings from R2 to 172.16.3.1  96
    Pings from R2 to 192.168.1.1  97
  Cisco Discovery Protocol (CDP)  99
    Network Discovery with CDP  99
    Layer 3 Neighbors  99
    Layer 2 Neighbors  100
    CDP Operation  101
Chapter 3  Introduction to Dynamic Routing Protocols  147

Objectives  147

Key Terms  147

Introduction to Dynamic Routing Protocols  148
  Perspective and Background  148
    Evolution of Dynamic Routing Protocols  149
    Role of Dynamic Routing Protocol  150
  Network Discovery and Routing Table Maintenance  151
    Purpose of Dynamic Routing Protocols  151
    Dynamic Routing Protocol Operation  151
  Dynamic Routing Protocol Advantages  152
    Static Routing Usage, Advantages, and Disadvantages  153
    Dynamic Routing Advantages and Disadvantages  153

Classifying Dynamic Routing Protocols  154
  IGP and EGP  154
  Distance Vector and Link-State Routing Protocols  156
    Distance Vector Routing Protocol Operation  156
    Link-State Protocol Operation  157
  Classful and Classless Routing Protocols  158
    Classful Routing Protocols  158
    Classless Routing Protocols  159
  Dynamic Routing Protocols and Convergence  159

Metrics  160
  Purpose of a Metric  160
  Metrics and Routing Protocols  161
    Metric Parameters  161
    Metric Field in the Routing Table  162
  Load Balancing  163
Administrative Distance 165

Purpose of Administrative Distance 165

Multiple Routing Sources 165

Purpose of Administrative Distance 165

Dynamic Routing Protocols and Administrative Distance 168

Static Routes and Administrative Distance 170

Directly Connected Networks and Administrative Distance 172

Summary 174

Activities and Labs 175

Check Your Understanding 175

Challenge Questions and Activities 178

To Learn More 178

Chapter 4 Distance Vector Routing Protocols 181

Objectives 181

Key Terms 181

Introduction to Distance Vector Routing Protocols 182

Distance Vector Technology 184

Meaning of Distance Vector 184

Operation of Distance Vector Routing Protocols 185

Routing Protocol Algorithms 186

Routing Protocol Characteristics 188

Comparing Routing Protocol Features 189

Network Discovery 190

Cold Start 190

Initial Exchange of Routing Information 191

Exchange of Routing Information 192

Convergence 194

Routing Table Maintenance 195

Periodic Updates 195

Maintaining the Routing Table 196

RIP Timers 196

Bounded Updates 198

Triggered Updates 198

Random Jitter 199
Routing Loops 200
Defining a Routing Loop 200
Implications of Routing Loops 201
Count-to-Infinity Condition 202
Preventing Routing Loops by Setting a Maximum Metric Value 203
Preventing Routing Loops with Hold-Down Timers 203
Preventing Routing Loops with the Split Horizon Rule 206
  Route Poisoning 207
  Split Horizon with Poison Reverse 208
Preventing Routing Loops with IP and TTL 209
Distance Vector Routing Protocols Today 210
  RIP and EIGRP 210
    RIP 211
    EIGRP 211
Summary 213
Activities and Labs 214
Check Your Understanding 214
Challenge Questions and Activities 217
To Learn More 218

Chapter 5  RIP Version 1 219
Objectives 219
Key Terms 219
RIPv1: Distance Vector, Classful Routing Protocol 220
  Background and Perspective 221
  RIPv1 Characteristics and Message Format 222
    RIP Characteristics 222
    RIP Message Format: RIP Header 222
    RIP Message Format: Route Entry 224
    Why Are So Many Fields Set to Zero? 224
  RIP Operation 224
    RIP Request/Response Process 225
    IP Address Classes and Classful Routing 225
  Administrative Distance 226
Basic RIPv1 Configuration 227
  RIPv1 Scenario A 227
  Enabling RIP: router rip Command 228
  Specifying Networks 229
Verification and Troubleshooting 231
Verifying RIP: show ip route Command 231
Verifying RIP: show ip protocols Command 233
Verifying RIP: debug ip rip Command 235
Passive Interfaces 236
  Unnecessary RIP Updates Impact Network 236
  Stopping Unnecessary RIP Updates 237

Automatic Summarization 238
Modified Topology: Scenario B 238
Boundary Routers and Automatic Summarization 242
Processing RIP Updates 243
  Rules for Processing RIPv1 Updates 243
  Example of RIPv1 Processing Updates 243
Sending RIP Updates: Using debug to View Automatic Summarization 244
Advantages and Disadvantages of Automatic Summarization 246
  Advantages of Automatic Summarization 246
  Disadvantage of Automatic Summarization 247
  Discontiguous Topologies Do Not Converge with RIPv1 248

Default Route and RIPv1 250
Modified Topology: Scenario C 250
  Propagating the Default Route in RIPv1 253

Summary 255
Activities and Labs 256
Check Your Understanding 257
Challenge Questions and Activities 260
To Learn More 262

Chapter 6 VLSM and CIDR 263
Objectives 263
Key Terms 263
Classful and Classless Addressing 264
Classful IP Addressing 265
  High-Order Bits 266
IPv4 Classful Addressing Structure 267
Classful Routing Protocol 268
Classless IP Addressing 269
  Moving Toward Classless Addressing 269
  CIDR and Route Summarization 270
Classless Routing Protocol 271

VLSM 272
  VLSM in Action 272
  VLSM and IP Addresses 275

CIDR 277
  Route Summarization 278
  Calculating Route Summarization 279

Summary 281
Activities and Labs 281
Check Your Understanding 283
Challenge Questions and Activities 286
To Learn More 288

Chapter 7  RIPv2 289
Objectives 289
Key Terms 289
RIPv1 Limitations 291
  Summary Route 295
  VLSM 295
  RFC 1918 Private Addresses 295
  Cisco Example IP Addresses 296
  Loopback Interfaces 297
  RIPv1 Topology Limitations 297
    Static Routes and Null Interfaces 298
    Route Redistribution 298
    Verifying and Testing Connectivity 298
  RIPv1: Discontiguous Networks 301
    Examining the Routing Tables 301
    How Classful Routing Protocols Determine Subnet Masks 304
  RIPv1: No VLSM Support 305
RIPv1: No CIDR Support 306
192.168.0.0/16 Static Route 307

**Configuring RIPv2** 309
- Enabling and Verifying RIPv2 309
- Auto-Summary and RIPv2 313
- Disabling Auto-Summary in RIPv2 315
- Verifying RIPv2 Updates 316

**VLSM and CIDR** 320
- RIPv2 and VLSM 320
- RIPv2 and CIDR 321

**Verifying and Troubleshooting RIPv2** 323
- Verification and Troubleshooting Commands 323
  - `show ip route Command` 323
  - `show ip interface brief Command` 324
  - `show ip protocols Command` 324
  - `debug ip rip Command` 325
  - `ping Command` 326
  - `show running-config Command` 327
- Common RIPv2 Issues 328
  - Authentication 328

**Summary** 330

**Activities and Labs** 330

**Check Your Understanding** 331

**Challenge Questions and Activities** 332

**To Learn More** 334

---

**Chapter 8** The Routing Table: A Closer Look 337

**Objectives** 337

**Key Terms** 337

**The Routing Table Structure** 338
- Lab Topology 338
- Routing Table Entries 340
- Level 1 Routes 341
- Parent and Child Routes: Classful Networks 344
  - *Level 1 Parent Route* 346
  - *Level 2 Child Route* 346
- Parent and Child Routes: Classless Networks 348
Basic OSPF Configuration  508
  Lab Topology  508
  The router ospf Command  512
  The network Command  512
  OSPF Router ID  513
    Determining the Router ID  514
    Highest Active IP Address  514
    Verifying the Router ID  514
    Loopback Address  515
    OSPF router-id Command  516
    Modifying the Router ID  516
    Duplicate Router IDs  517
  Verifying OSPF  518
  Examining the Routing Table  522

The OSPF Metric  523
  OSPF Metric  524
    Reference Bandwidth  524
    OSPF Accumulates Cost  524
    Default Bandwidth on Serial Interfaces  525
  Modifying the Cost of the Link  527
    The bandwidth Command  527
    The ip ospf cost Command  528
    The bandwidth Command vs. the ip ospf cost Command  529

OSPF and Multiaccess Networks  530
  Challenges in Multiaccess Networks  530
    Multiple Adjacencies  531
    Flooding of LSAs  533
    Solution: Designated Router  534
  DR/BDR Election Process  536
    Topology Change  536
    DR/BDR Election  537
    Timing of DR/BDR Election  539
  OSPF Interface Priority  542

More OSPF Configuration  545
  Redistributing an OSPF Default Route  545
    Topology  545
  Fine-Tuning OSPF  548
    Reference Bandwidth  548
    Modifying OSPF Intervals  550
Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the 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** indicate 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 Cisco Networking Academy is a comprehensive e-learning program that provides students with Internet technology skills. A Networking Academy delivers web-based content, online assessment, student performance tracking, and hands-on labs to prepare students for industry-standard certifications. The CCNA curriculum includes four courses oriented around the topics of the Cisco Certified Network Associate (CCNA) certification.

*Routing Protocols and Concepts, CCNA Exploration Companion Guide* is the official supplement textbook to be used with v4 of the CCNA Exploration Routing Protocols and Concepts online curriculum of the Networking Academy.

This book goes beyond earlier editions of the Cisco Press *Companion Guides* by providing many alternate explanations and examples as compared to the course. You can use the online curriculum as normal and use this companion guide to help solidify your understanding of all the topics through the alternate examples.

The basis for this book as well as the online curriculum is to provide you with a thorough understanding of routing protocols and concepts beyond that necessary for the CCNA certification exam. The commands used for configuring routing protocols are not very difficult. The challenge is to understand the operation of those protocols and their effect upon the network.

The objective of this book is to explain routing protocols and concepts. Every concept is methodically explained with no assumptions made of the reader’s knowledge of routing protocols. The only exceptions are, if a concept is beyond the scope of this course or is covered in CCNP, it is noted within the text.

Readers are welcome to use the resources on Rick Graziani’s website: http://www.cabrillo.edu/~rgraziani. You can e-mail Rick Graziani at graziani@cabrillo.edu to obtain the username and password to access his resources for this course and all other CCNA and CCNP courses, including PowerPoint presentations.

Goal of This Book

First and foremost, by providing a fresh, complementary perspective on the content, this book is intended to help you learn all the required materials of the Routing Protocols and Concepts course in the Networking Academy CCNA Exploration curriculum. As a secondary goal, the text is intended as a mobile replacement for the online curriculum for individuals who do not always have Internet access. In those cases, you can instead read the appropriate sections of the book, as directed by your instructor, and learn the same material that is covered in the online curriculum. Another secondary goal is to serve as your offline study material to prepare for the CCNA exam.
Audience for This Book

This book’s main audience is anyone taking the CCNA Exploration Routing Protocols and Concepts course of the Cisco Networking Academy curriculum. Many Academies use this textbook as a required tool in the course, while other Academies recommend the Companion Guides as an additional source of study and practice materials.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives**—Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the Companion Guide encourages you to think about finding the answers as you read the chapter.

- **“How-to” feature:** When this book covers a set of steps that you need to perform for certain tasks, it lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.

- **Notes, tips, cautions, and warnings:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.

- **Chapter summaries:** At the end of each chapter is a summary of the chapter’s key concepts. It provides a synopsis of the chapter and serves as a study aid.

Readability

The authors have compiled, edited, and in some cases, rewritten the material so that it has a more conversational tone that follows a consistent and accessible reading level. In addition, the following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.

- **Glossary:** This book contains an all-new Glossary, with more than 150 terms.
Practice

Practice makes perfect. This new Companion Guide offers you ample opportunities to put what you learn to practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key**: Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. The appendix, “Check Your Understanding and Challenge Questions Answer Key,” provides an answer key to all the questions and includes an explanation of each answer.

- **(NEW) Challenge questions and activities**: Additional—and more challenging—review questions and activities are presented at the end of chapters. These questions are purposefully designed to be similar to the more complex styles of questions you might see on the CCNA exam. This section might also include activities to help prepare you for the exams. The appendix provides the answers.

- **Packet Tracer Activities**: Interspersed throughout the chapters, you’ll find many activities that allow you to work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available on this book’s CD-ROM; Packet Tracer software, however, is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.

Labs and Study Guide


- **Lab and Activity references**: This icon notes the hands-on labs and other activities created for this chapter in the online curriculum. Within *Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide*, you will also find additional labs and study guide material created by the author of that book.

- **(NEW) Packet Tracer Companion activities**: Many of the hands-on labs include Packet Tracer Companion activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in *Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide*, by Cisco Press (ISBN 1-58713-204-4), for hands-on labs that have a Packet Tracer Companion.
(NEW) Packet Tracer Skills Integration Challenge activities: These activities require you to pull together several skills learned from the chapter to successfully complete one comprehensive exercise. Look for this icon in *Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide*, by Cisco Press (ISBN 1-58713-204-4) for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.

**A Word About Packet Tracer Software and Activities**

Packet Tracer is a self-paced, visual interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This “e-doing” capability is a fundamental component of learning how to configure routers and switches from the command line.

Packet Tracer v4.x is available only to Cisco Networking Academies through the Academy Connection website. Ask your instructor for access to Packet Tracer.

The course includes essentially three different types of Packet Tracer activities. This book uses an icon system to indicate which type of Packet Tracer activity is available. The icons are intended to give you a sense of the purpose of the activity and the amount of time you need to allot to complete it. The three types of Packet Tracer activities follow:

- **Packet Tracer Activity**: This icon identifies straightforward exercises interspersed throughout the chapters where you can practice or visualize a specific topic. The activity files for these exercises are available on this book’s CD-ROM. These activities take less time to complete than the Packet Tracer Companion and Challenge activities.

- **Packet Tracer Companion**: This icon identifies exercises that correspond to the hands-on labs of the course. You can use Packet Tracer to complete a simulation of the hands-on lab or complete a similar “lab.” The Companion Guide points these out at the end of each chapter, but look for this icon and the associated exercise file in *Routing Protocols and Concepts CCNA Exploration Labs and Study Guide* for hands-on labs that have a Packet Tracer Companion.

- **Packet Tracer Skills Integration Challenge**: This icon identifies activities that require you to pull together several skills learned from the chapter to successfully complete one comprehensive exercise. The *Companion Guide* points these out at the end of each
chapter, but look for this icon in *Routing Protocols and Concepts CCNA Exploration Labs and Study Guide* for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.

**How This Book Is Organized**

The book covers the major topic headings in the same sequence as the online curriculum for the CCNA Exploration Routing Protocols and Concepts course. This book has 11 chapters, with the same numbers and similar names as the online course chapters.

Each routing protocol chapter and the static routing chapter begin with a single topology that is used throughout the chapter. The single topology per chapter allows better continuity and easier understanding of routing commands, operations, and outputs.

- **Chapter 1, “Introduction to Routing and Packet Forwarding,”** provides an overview of the router hardware and software, along with an introduction to directly connected networks, static routing, and dynamic routing protocols. The process of packet forwarding is also reviewed, including the path determination and switching functions.

- **Chapter 2, “Static Routing,”** examines static routing in detail. The use of static routes and the role they play in modern networks are discussed. This chapter describes the advantages, uses, and configuration of static routes using next-hop IP addresses and/or exit interfaces. Basic Cisco IOS commands are reviewed, along with an introduction to the Cisco IP routing table.

- **Chapter 3, “Introduction to Dynamic Routing Protocols,”** provides an overview of dynamic routing protocols and the various methods used to classify them. The terms *metrics* and *administrative distance* are introduced. This chapter serves as an introduction to terms and concepts that are examined more fully in later chapters.

- **Chapter 4, “Distance Vector Routing Protocols,”** covers the theory behind distance vector routing protocols. The algorithm used by distance vector routing protocols, along with the process of network discovery and routing table maintenance, is discussed.

- **Chapter 5, “RIP Version 1,”** examines the distance vector routing protocol RIPv1. Although it is the oldest IP routing protocol, RIPv1 is the ideal candidate for discussing distance vector technology and classful routing protocols. This chapter includes the configuration, verification, and troubleshooting of RIPv1.

- **Chapter 6, “VLSM and CIDR,”** discusses VLSM (variable-length subnet masks) and CIDR (classless interdomain routing), including how to allocate IP addresses according to need rather than by class, and how IP addresses can be summarized as a single address, which is known as *supernetting.*
Chapter 7, “RIPv2,” discusses RIPv2, a distance vector routing protocol. RIPv2 is a classless routing protocol as compared to RIPv1, which is a classful routing protocol. This chapter examines the benefits of using a classless routing protocol and describes how it supports both VLSM and CIDR. This chapter includes the configuration, verification, and troubleshooting of RIPv2.

Chapter 8, “The Routing Table: A Closer Look,” examines the Cisco IPv4 routing table in detail. Understanding the structure and lookup process of the routing table provides a valuable tool in verifying and troubleshooting networks.

Chapter 9, “EIGRP,” discusses the classless routing protocol EIGRP. EIGRP is a Cisco-proprietary, advanced distance vector routing protocol. This chapter examines DUAL (Diffusing Update Algorithm) and describes how DUAL determines best paths and loop-free backup paths. This chapter includes the configuration, verification, and troubleshooting of EIGRP.

Chapter 10, “Link-State Routing Protocols,” provides an introduction to link-state terms and concepts. This chapter compares link-state and distance vector routing protocols, discussing the benefits and requirements of using a link-state routing protocol.

Chapter 11, “OSPF,” examines the classless, link-state routing protocol OSPF. OSPF operations are discussed, including link-state updates, adjacency, and the DR/BDR election process. This chapter includes the configuration, verification, and troubleshooting of OSPF.

Appendix, “Check Your Understanding and Challenge Questions Answer Key,” provides the answers to the Check Your Understanding questions that you find at the end of each chapter. It also includes answers for the Challenge Questions and Activities that conclude most chapters.

The Glossary provides a compiled list of all the key terms that appear throughout this book.

About the CD-ROM

The CD-ROM included with this book provides many useful tools and information to support your education:

- Packet Tracer Activity files: These are files to work through the Packet Tracer Activities referenced throughout the book, as indicated by the Packet Tracer Activity icon.

- Taking Notes: This section includes a .txt file of the chapter objectives to serve as a general outline of the key topics of which you need to take note. The practice of taking clear, consistent notes is an important skill not only for learning and studying the material but for on-the-job success as well. Also included in this section is “A Guide to Using a Networker’s Journal” PDF booklet providing important insight into the value
of the practice of using a journal, how to organize a professional journal, and some best practices on what, and what not, to take note of in your journal.

■ **IT Career Information:** This section includes a student guide to applying the toolkit approach to your career development. Learn more about entering the world of Information Technology as a career by reading two informational chapters excerpted from *The IT Career Builder’s Toolkit*: “Defining Yourself: Aptitudes and Desires” and “Making Yourself Indispensable.”

■ **Lifelong Learning in Networking:** As you embark on a technology career, you will notice that it is ever-changing and evolving. This career path provides new and exciting opportunities to learn new technologies and their applications. Cisco Press is one of the key resources to plug into on your quest for knowledge. This section of the CD-ROM provides an orientation to the information available to you and tips on how to tap into these resources for lifelong learning.
CHAPTER 3

Introduction to Dynamic Routing Protocols

Objectives

Upon completion of this chapter, you should be able to answer the following questions:

■ Can you describe the role of dynamic routing protocols and place these protocols in the context of modern network design?

■ What are several ways to classify routing protocols?

■ How are metrics used by routing protocols, and what are the metric types used by dynamic routing protocols?

■ How do you determine the administrative distance of a route, and what is its importance in the routing process?

■ What are the different elements in the routing table?

■ Given realistic constraints, can you devise and apply subnetting schemes?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary at the end of the book.

scale  page 149
algorithm  page 151
autonomous system  page 154
routing domain  page 154
interior gateway protocols  page 154
exterior gateway protocols  page 154
path vector protocol  page 156
distance vector  page 156
vectors  page 156
link-state  page 157
link-state router  page 157
converged  page 157
classful routing protocols  page 158
VLSM  page 158
discontiguous  page 158
classless routing protocols  page 159
convergence  page 159
administrative distance  page 165
The data networks that we use in our everyday lives to learn, play, and work range from small, local networks to large, global internetworks. At home, you might have a router and two or more computers. At work, your organization might have multiple routers and switches servicing the data communication needs of hundreds or even thousands of PCs.

In Chapters 1 and 2, you discovered how routers are used in packet forwarding and that routers learn about remote networks using both static routes and dynamic routing protocols. You also know how routes to remote networks can be configured manually using static routes.

This chapter introduces dynamic routing protocols, including how different routing protocols are classified, what metrics they use to determine best path, and the benefits of using a dynamic routing protocol.

Dynamic routing protocols are typically used in larger networks to ease the administrative and operational overhead of using only static routes. Typically, a network uses a combination of both a dynamic routing protocol and static routes. In most networks, a single dynamic routing protocol is used; however, there are cases where different parts of the network can use different routing protocols.

Since the early 1980s, several different dynamic routing protocols have emerged. This chapter begins to discuss some of the characteristics and differences in these routing protocols; however, this will become more evident in later chapters, with a discussion of several of these routing protocols in detail.

Although many networks will use only a single routing protocol or use only static routes, it is important for a network professional to understand the concepts and operations of all the different routing protocols. A network professional must be able to make an informed decision regarding when to use a dynamic routing protocol and which routing protocol is the best choice for a particular environment.

**Introduction to Dynamic Routing Protocols**

Dynamic routing protocols play an important role in today’s networks. The following sections describe several important benefits that dynamic routing protocols provide. In many networks, dynamic routing protocols are typically used with static routes.

**Perspective and Background**

Dynamic routing protocols have evolved over several years to meet the demands of changing network requirements. Although many organizations have migrated to more recent routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), many of the earlier routing protocols, such as Routing Information Protocol (RIP), are still in use today.
Evolution of Dynamic Routing Protocols

Dynamic routing protocols have been used in networks since the early 1980s. The first version of RIP was released in 1982, but some of the basic algorithms within the protocol were used on the ARPANET as early as 1969.

As networks have evolved and become more complex, new routing protocols have emerged. Figure 3-1 shows the classification of routing protocols.

Figure 3-1  Routing Protocols' Evolution and Classification

<table>
<thead>
<tr>
<th>Classful</th>
<th>Classless</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP</td>
<td>IGRP</td>
<td>RIPng</td>
</tr>
<tr>
<td>EGP</td>
<td>IGRP</td>
<td>OSPFv3</td>
</tr>
<tr>
<td>1982</td>
<td>1985</td>
<td>1991</td>
</tr>
<tr>
<td>1985</td>
<td>1988</td>
<td>1990</td>
</tr>
<tr>
<td>1988</td>
<td>1990</td>
<td>1994</td>
</tr>
<tr>
<td>1992</td>
<td>1995</td>
<td>1999</td>
</tr>
<tr>
<td>1995</td>
<td>1997</td>
<td>2000</td>
</tr>
</tbody>
</table>

Highlighted routing protocols are the focus of this course.

Figure 3-1 shows a timeline of IP routing protocols, with a chart that helps classify the various protocols. This chart will be referred to several times throughout this book.

One of the earliest routing protocols was RIP. RIP has evolved into a newer version: RIPv2. However, the newer version of RIP still does not scale to larger network implementations.

To address the needs of larger networks, two advanced routing protocols were developed: OSPF and Intermediate System–to–Intermediate System (IS-IS). Cisco developed Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP). EIGRP also scales well in larger network implementations.

Additionally, there was the need to interconnect different internetworks and provide routing among them. Border Gateway Protocol (BGP) is now used between Internet service providers (ISP) as well as between ISPs and their larger private clients to exchange routing information.

With the advent of numerous consumer devices using IP, the IPv4 addressing space is nearly exhausted. Thus IPv6 has emerged. To support the communication based on IPv6, newer versions of the IP routing protocols have been developed (see the IPv6 row in Figure 3-1).
Note
This chapter presents an overview of the different dynamic routing protocols. More details about RIP, EIGRP, and OSPF routing protocols will be discussed in later chapters. The IS-IS and BGP routing protocols are explained in the CCNP curriculum. IGRP is the predecessor to EIGRP and is now considered obsolete.

Role of Dynamic Routing Protocol
What exactly are dynamic routing protocols? Routing protocols are used to facilitate the exchange of routing information between routers. Routing protocols allow routers to dynamically learn information about remote networks and automatically add this information to their own routing tables, as shown in Figure 3-2.

Figure 3-2   Routers Dynamically Pass Updates

Routing protocols determine the best path to each network, which is then added to the routing table. One of the primary benefits of using a dynamic routing protocol is that routers exchange routing information whenever there is a topology change. This exchange allows routers to automatically learn about new networks and also to find alternate paths if there is a link failure to a current network.

Compared to static routing, dynamic routing protocols require less administrative overhead. However, the expense of using dynamic routing protocols is dedicating part of a router’s resources for protocol operation, including CPU time and network link bandwidth. Despite the benefits of dynamic routing, static routing still has its place. There are times when static routing is more appropriate and other times when dynamic routing is the better choice. More often than not, you will find a combination of both types of routing in any network that has a moderate level of complexity. You will learn about the advantages and disadvantages of static and dynamic routing later in this chapter.
Network Discovery and Routing Table Maintenance

Two important processes concerning dynamic routing protocols are initially discovering remote networks and maintaining a list of those networks in the routing table.

Purpose of Dynamic Routing Protocols

A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol’s choice of best paths. The purpose of a routing protocol includes

■ Discovering remote networks
■ Maintaining up-to-date routing information
■ Choosing the best path to destination networks
■ Having the ability to find a new best path if the current path is no longer available

The components of a routing protocol are as follows:

■ **Data structures:** Some routing protocols use tables or databases for their operations. This information is kept in RAM.

■ **Algorithm:** An *algorithm* is a finite list of steps used in accomplishing a task. Routing protocols use algorithms for processing routing information and for best-path determination.

■ **Routing protocol messages:** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and do other tasks to learn and maintain accurate information about the network.

Dynamic Routing Protocol Operation

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 depends on the algorithm it uses and the operational characteristics of that protocol. The operations of a dynamic routing protocol vary depending on the type of routing protocol and the specific operations of that routing protocol. The specific operations of RIP, EIGRP, and OSPF are examined in later chapters. In general, the operations of a dynamic routing protocol can be described as follows:

1. The router sends and receives routing messages on its interfaces.
2. The router shares routing messages and routing information with other routers that are using the same routing protocol.
3. Routers exchange routing information to learn about remote networks.
4. When a router detects a topology change, the routing protocol can advertise this change to other routers.

**Dynamic Routing Protocol Advantages**

Dynamic routing protocols provide several advantages, which will be discussed in this section. In many cases, the complexity of the network topology, the number of networks, and the need for the network to automatically adjust to changes require the use of a dynamic routing protocol.

Before examining the benefits of dynamic routing protocols in more detail, you need to consider the reasons why you would use static routing. Dynamic routing certainly has several advantages over static routing; however, static routing is still used in networks today. In fact, networks typically use a combination of both static and dynamic routing.

Table 3-1 compares dynamic and static routing features. From this comparison, you can list the advantages of each routing method. The advantages of one method are the disadvantages of the other.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Dynamic Routing</th>
<th>Static Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Generally independent of the network size</td>
<td>Increases with network size</td>
</tr>
<tr>
<td>complexity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required administrator knowledge</td>
<td>Advanced knowledge required</td>
<td>No extra knowledge required</td>
</tr>
<tr>
<td>Topology changes</td>
<td>Automatically adapts to topology changes</td>
<td>Administrator intervention required</td>
</tr>
<tr>
<td>Scaling</td>
<td>Suitable for simple and complex topologies</td>
<td>Suitable for simple topologies</td>
</tr>
<tr>
<td>Security</td>
<td>Less secure</td>
<td>More secure</td>
</tr>
<tr>
<td>Resource usage</td>
<td>Uses CPU, memory, and link bandwidth</td>
<td>No extra resources needed</td>
</tr>
<tr>
<td>Predictability</td>
<td>Route depends on the current topology</td>
<td>Route to destination is always the same</td>
</tr>
</tbody>
</table>
Static Routing Usage, Advantages, and Disadvantages

Static routing has several primary uses, including the following:

- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from stub networks (see Chapter 2).
- Using a single default route, used to represent a path to any network that does not have a more specific match with another route in the routing table.

Static routing advantages are as follows:

- Minimal CPU processing
- Easier for administrator to understand
- Easy to configure

Static routing disadvantages are as follows:

- Configuration and maintenance are time-consuming.
- Configuration is error-prone, especially in large networks.
- Administrator intervention is required to maintain changing route information.
- Does not scale well with growing networks; maintenance becomes cumbersome.
- Requires complete knowledge of the entire network for proper implementation.

Dynamic Routing Advantages and Disadvantages

Dynamic routing advantages are as follows:

- Administrator has less work in maintaining the configuration when adding or deleting networks.
- Protocols automatically react to the topology changes.
- Configuration is less error-prone.
- More scalable; growing the network usually does not present a problem.

Dynamic routing disadvantages are as follows:

- Router resources are used (CPU cycles, memory, and link bandwidth).
- More administrator knowledge is required for configuration, verification, and troubleshooting.
Classifying Dynamic Routing Protocols

Figure 3-1 showed how routing protocols can be classified according to various characteristics. This chapter will introduce you to these terms, which will be discussed in more detail in later chapters.

This section gives an overview of the most common IP routing protocols. Most of these routing protocols will be examined in detail later in this book. For now, we will give a very brief overview of each protocol.

Routing protocols can be classified into different groups according to their characteristics:

- IGP or EGP
- Distance vector or link-state
- Classful or classless

The sections that follow discuss these classification schemes in more detail.

The most commonly used routing protocols are as follows:

- **RIP**: A distance vector interior routing protocol
- **IGRP**: The distance vector interior routing protocol developed by Cisco (deprecated from Cisco IOS Release 12.2 and later)
- **OSPF**: A link-state interior routing protocol
- **IS-IS**: A link-state interior routing protocol
- **EIGRP**: The advanced distance vector interior routing protocol developed by Cisco
- **BGP**: A path vector exterior routing protocol

*Note*

IS-IS and BGP are beyond the scope of this book.

IGP and EGP

An *autonomous system* (AS)—otherwise known as a *routing domain*—is a collection of routers under a common administration. Typical examples are a company’s internal network and an ISP’s network. Because the Internet is based on the autonomous system concept, two types of routing protocols are required: interior and exterior routing protocols. These protocols are

- **Interior gateway protocols (IGP)**: Used for intra-autonomous system routing, that is, routing inside an autonomous system
- **Exterior gateway protocols (EGP)**: Used for inter-autonomous system routing, that is, routing between autonomous systems
Figure 3-3 is a simplified view of the difference between IGPs and EGPs. The autonomous system concept will be explained in more detail later in the chapter. Even though this is an oversimplification, for now, think of an autonomous system as an ISP.

**Figure 3-3**  IGP Versus EGP Routing Protocols

IGPs are used for routing within a routing domain, those networks within the control of a single organization. An autonomous system is commonly composed of many individual networks belonging to companies, schools, and other institutions. An IGP is used to route within the autonomous system and also used to route within the individual networks themselves. For example, The Corporation for Education Network Initiatives in California (CENIC) operates an autonomous system composed of California schools, colleges, and universities. CENIC uses an IGP to route within its autonomous system to interconnect all of these institutions. Each of the educational institutions also uses an IGP of its own choosing to route within its own individual network. The IGP used by each entity provides best-path determination within its own routing domains, just as the IGP used by CENIC provides best-path routes within the autonomous system itself. IGPs for IP include RIP, IGRP, EIGRP, OSPF, and IS-IS.

Routing protocols (and more specifically, the algorithm used by that routing protocol) use a metric to determine the best path to a network. The metric used by the routing protocol RIP is *hop count*, which is the number of routers that a packet must traverse in reaching another network. OSPF uses *bandwidth* to determine the shortest path.
EGPs, on the other hand, are designed for use between different autonomous systems that are under the control of different administrations. BGP is the only currently viable EGP and is the routing protocol used by the Internet. BGP is a *path vector protocol* that can use many different attributes to measure routes. At the ISP level, there are often more important issues than just choosing the fastest path. BGP is typically used between ISPs and sometimes between a company and an ISP. BGP is not part of this course or CCNA; it is covered in CCNP.

**Characteristics of IGP and EGP Routing Protocols (3.2.2)**

In this activity, the network has already been configured within the autonomous systems. You will configure a default route from AS2 and AS3 (two different companies) to the ISP (AS1) to simulate the exterior gateway routing that would take place from both companies to their ISP. Then you will configure a static route from the ISP (AS1) to AS2 and AS3 to simulate the exterior gateway routing that would take place from the ISP to its two customers, AS2 and AS3. View the routing table before and after both static routes and default routes are added to observe how the routing table has changed. Use file e2-322.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

**Distance Vector and Link-State Routing Protocols**

Interior gateway protocols (IGP) can be classified as two types:

- Distance vector routing protocols
- Link-state routing protocols

**Distance Vector Routing Protocol Operation**

*Distance vector* means that routes are advertised as *vectors* of distance and direction. Distance is defined in terms of a metric such as hop count, and direction is simply the next-hop router or exit interface. Distance vector protocols typically use the Bellman-Ford algorithm for the best-path route determination.

Some distance vector protocols periodically send complete routing tables to all connected neighbors. In large networks, these routing updates can become enormous, causing significant traffic on the links.

Although the Bellman-Ford algorithm eventually accumulates enough knowledge to maintain a database of reachable networks, the algorithm does not allow a router to know the exact topology of an internetwork. The router only knows the routing information received from its neighbors.

Distance vector protocols use routers as signposts along the path to the final destination. The only information 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.

Distance vector protocols work best in situations where

- The network is simple and flat and does not require a hierarchical design.
- The administrators do not have enough knowledge to configure and troubleshoot link-state protocols.
- Specific types of networks, such as hub-and-spoke networks, are being implemented.
- Worst-case convergence times in a network are not a concern.

Chapter 4, “Distance Vector Routing Protocols,” covers distance vector routing protocol functions and operations in greater detail. You will also learn about the operations and configuration of the distance vector routing protocols RIP and EIGRP.

**Link-State Protocol Operation**

In contrast to distance vector routing protocol operation, a router configured with a link-state routing protocol can create a “complete view,” or topology, of the network by gathering information from all the other routers. Think of using a link-state routing protocol as having a complete map of the network topology. The signposts along the way from source to 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 to select the best path to all destination networks in the topology.

With some distance vector routing protocols, routers send periodic updates of their routing information to their neighbors. Link-state routing protocols do not use periodic updates. After the network has converged, a link-state update is only sent when there is a change in the topology.

Link-state protocols work best in situations where

- The network design is hierarchical, usually occurring in large networks.
- The administrators have a good knowledge of the implemented link-state routing protocol.
- Fast convergence of the network is crucial.

Link-state routing protocol functions and operations will be explained in later chapters. You will also learn about the operations and configuration of the link-state routing protocol OSPF in Chapter 11, “OSPF.”
Classful and Classless Routing Protocols

All routing protocols can also be classified as either

- Classful routing protocols
- Classless routing protocols

Classful Routing Protocols

*Classful routing protocols* do not send subnet mask information in routing updates. The first routing protocols, such as RIP, were classful. This was at a time when network addresses were allocated based on classes: Class A, B, or C. A routing protocol did not need to include the subnet mask in the routing update because the network mask could be determined based on the first octet of the network address.

Classful routing protocols can still be used in some of today’s networks, but because they do not include the subnet mask, they cannot be used in all situations. Classful routing protocols cannot be used when a network is subnetted using more than one subnet mask. In other words, classful routing protocols do not support variable-length subnet masks (*VLSM*).

Figure 3-4 shows an example of a network using the same subnet mask on all its subnets for the same major network address. In this situation, either a classful or classless routing protocol could be used.

**Figure 3-4** Classful Routing

There are other limitations to classful routing protocols, including their inability to support *discontiguous* networks. Later chapters discuss classful routing protocols, discontiguous networks, and VLSM in greater detail.

Classful routing protocols include RIPv1 and IGRP.
Classless Routing Protocols

*Classless routing protocols* include the subnet mask with the network address in routing updates. Today’s networks are no longer allocated based on classes, and the subnet mask cannot be determined by the value of the first octet. Classless routing protocols are required in most networks today because of their support for VLSM, discontiguous networks, and other features that will be discussed in later chapters.

In Figure 3-5, notice that the classless version of the network is using both /30 and /27 subnet masks in the same topology. Also notice that this topology is using a discontiguous design.

Classless routing protocols are RIPv2, EIGRP, OSPF, IS-IS, and BGP.

**Dynamic Routing Protocols and Convergence**

An important characteristic of a routing protocol is how quickly it converges when there is a change in the topology.

*Convergence* is when the routing tables of all routers are at a state of consistency. The network has converged when all routers have complete and accurate information about the network. Convergence time is the time it takes routers to share information, calculate best paths, and update their routing tables. A network is not completely operable until the network has converged; therefore, most networks require short convergence times.

Convergence is both collaborative and independent. The routers share information with each other but must independently calculate the impacts of the topology change on their own routes. Because they develop an agreement with the new topology independently, they are said to *converge* on this consensus.
Convergence properties include the speed of propagation of routing information and the calculation of optimal paths. Routing protocols can be rated based on the speed to convergence; the faster the convergence, the better the routing protocol. Generally, RIP and IGRP are slow to converge, whereas EIGRP, OSPF, and IS-IS are faster to converge.

**Convergence (3.2.5)**

In this activity, the network has already been configured with two routers, two switches, and two hosts. A new LAN will be added, and you will watch the network converge. Use file e2-325.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

---

**Metrics**

Metrics are a way to measure or compare. Routing protocols use metrics to determine which route is the best path.

**Purpose of a Metric**

There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and differentiate among the available paths. For this purpose, a metric is used. A metric is a value used by routing protocols to assign costs to reach remote networks. The metric is used to determine which path is most preferable when there are multiple paths to the same remote network.

Each routing protocol calculates its metric in a different way. For example, RIP uses hop count, EIGRP uses a combination of bandwidth and delay, and the Cisco implementation of OSPF uses bandwidth. Hop count is the easiest metric to envision. The hop count refers to the number of routers a packet must cross to reach the destination network.

For Router R3 in Figure 3-6, network 172.16.3.0 is two hops, or two routers, away. For Router R2, network 172.16.3.0 is one hop away, and for Router R1, it is 0 hops (because the network is directly connected).

**Note**

The metrics for a particular routing protocol and a discussion of how they are calculated will be presented in the chapter for that routing protocol.
Metrics and Routing Protocols

Different routing protocols use different metrics. The metric used by one routing protocol is not comparable to the metric used by another routing protocol.

Metric Parameters

Two different routing protocols might choose different paths to the same destination because of using different metrics.

Figure 3-7 shows how R1 would reach the 172.16.3.0/24 network. RIP would choose the path with the least amount of hops through R2, whereas OSPF would choose the path with the highest bandwidth through R3.

Metrics used in IP routing protocols include the following:

- **Hop count**: A simple metric that counts the number of routers a packet must traverse.
- **Bandwidth**: Influences path selection by preferring the path with the highest bandwidth.
- **Load**: Considers the traffic utilization of a certain link.
- **Delay**: Considers the time a packet takes to traverse a path.
- **Reliability**: Assesses the probability of a link failure, calculated from the interface error count or previous link failures.
- **Cost**: A value determined either by the IOS or by the network administrator to indicate preference for a route. Cost can represent a metric, a combination of metrics, or a policy.
At this point, it is not important to completely understand these metrics; they will be explained in later chapters.

**Metric Field in the Routing Table**

The routing table displays the metric for each dynamic and static route. Remember from Chapter 2 that static routes always have a metric of 0.

The list that follows defines the metric for each routing protocol:

- **RIP: Hop count:** Best path is chosen by the route with the lowest hop count.
- **IGRP and EIGRP: Bandwidth, delay, reliability, and load:** Best path is chosen by the route with the smallest composite metric value calculated from these multiple parameters. By default, only bandwidth and delay are used.
- **IS-IS and OSPF: Cost:** Best path is chosen by the route with the lowest cost. The Cisco implementation of OSPF uses bandwidth to determine the cost. IS-IS is discussed in CCNP.

Routing protocols determine best path based on the route with the lowest metric.

In Figure 3-8, all the routers are using the RIP routing protocol.

The metric associated with a certain route can be best viewed using the `show ip route` command. The metric value is the second value in the brackets for a routing table entry. In Example 3-1, R2 has a route to the 192.168.8.0/24 network that is two hops away. The highlighted 2 in the command output is where the routing metric is displayed.
Load Balancing

You now know that individual routing protocols use metrics to determine the best route to reach remote networks. But what happens when two or more routes to the same destination have identical metric values? How will the router decide which path to use for packet forwarding? In this case, the router does not choose only one route. Instead, the router load-balances between these equal-cost paths. The packets are forwarded using all equal-cost paths.

Example 3-1 Routing Table for R2

R2# show ip route

<output omitted>

Gateway of last resort is not set

R  192.168.1.0/24  [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
C  192.168.2.0/24  is directly connected, Serial0/0/0
C  192.168.3.0/24  is directly connected, FastEthernet0/0
C  192.168.4.0/24  is directly connected, Serial0/0/1
R  192.168.5.0/24  [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
R  192.168.6.0/24  [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
   [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
R  192.168.7.0/24  [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
R  192.168.8.0/24  [120/2] via 192.168.4.1, 00:00:26, Serial0/0/1
To see whether load balancing is in effect, check the routing table. Load balancing is in effect if two or more routes are associated with the same destination.

**Note**

Load balancing can be done either per packet or per destination. How a router actually load-balances packets between the equal-cost paths is governed by the switching process. The switching process will be discussed in greater detail in a later chapter.

Figure 3-9 shows an example of load balancing, assuming that R2 load-balances traffic to PC5 over two equal-cost paths.

**Figure 3-9** Load Balancing Across Equal-Cost Paths

![Diagram](image)

R2 load balances traffic destined for the 192.168.6.0/24 network.

The `show ip route` command in Example 3-1 reveals that the destination network 192.168.6.0 is available through 192.168.2.1 (Serial 0/0/0) and 192.168.4.1 (Serial 0/0/1). The equal-cost routes are shown again here:

```
R2# show ip route

<output omitted>
R 192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
   [120/1] via 192.168.4.1, 00:00:26, Serial0/0/1
```

All the routing protocols discussed in this course are capable of automatically load-balancing traffic for up to four equal-cost routes by default. EIGRP is also capable of load-balancing across unequal-cost paths. This feature of EIGRP is discussed in the CCNP courses.
Administrative Distance

The following sections introduce the concept of administrative distance. Administrative
distance will also be discussed within each chapter that focuses on a particular routing
protocol.

Purpose of Administrative Distance

Before the routing process can determine which route to use when forwarding a packet, it
must first determine which routes to include in the routing table. There can be times when a
router learns a route to a remote network from more than one routing source. The routing
process will need to determine which routing source to use. **Administrative distance** is used
for this purpose.

Multiple Routing Sources

You know that routers learn about adjacent networks that are directly connected and about
remote networks by using static routes and dynamic routing protocols. In fact, a router
might learn of a route to the same network from more than one source. For example, a stat-
ic route might have been configured for the same network/subnet mask that was learned
dynamically by a dynamic routing protocol, such as RIP. The router must choose which
route to install.

**Note**

You might be wondering about equal-cost paths. Multiple routes to the same network can only be
installed when they come from the same routing source. For example, for equal-cost routes to be
installed, they both must be static routes or they both must be RIP routes.

Although less common, more than one dynamic routing protocol can be deployed in the
same network. In some situations, it might be necessary to route the same network address
using multiple routing protocols such as RIP and OSPF. Because different routing protocols
use different metrics—RIP uses hop count and OSPF uses bandwidth—it is not possible to
compare metrics to determine the best path.

So, how does a router determine which route to install in the routing table when it has
learned about the same network from more than one routing source? Cisco IOS makes the
determination based on the administrative distance of the routing source.

Purpose of Administrative Distance

Administrative distance (AD) defines the preference of a routing source. Each routing
source—including specific routing protocols, static routes, and even directly connected
networks—is prioritized in order of most to least preferable using an administrative distance
value. Cisco routers use the AD feature to select the best path when they learn about the
same destination network from two or more different routing sources.
Administrative distance is an integer value from 0 to 255. The lower the value, the more preferred the route source. An administrative distance of 0 is the most preferred. Only a directly connected network has an administrative distance of 0, which cannot be changed.

**Note**
It is possible to modify the administrative distance for static routes and dynamic routing protocols. This is discussed in CCNP courses.

An administrative distance of 255 means the router will not believe the source of that route, and it will not be installed in the routing table.

**Note**
The term *trustworthiness* is commonly used when defining administrative distance. The lower the administrative distance value, the more trustworthy the route.

Figure 3-10 shows a topology with R2 running both EIGRP and RIP. R2 is running EIGRP with R1 and RIP with R3.

**Figure 3-10  Comparing Administrative Distances**

Example 3-2 displays the `show ip route` command output for R2.
Example 3-2  Routing Table for R2

R2# show ip route

<output omitted>

Gateway of last resort is not set

D 192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0
C 192.168.2.0/24 is directly connected, Serial0/0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/0
C 192.168.4.0/24 is directly connected, Serial0/0/1
R 192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D 192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R 192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R 192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1

The AD value is the first value in the brackets for a routing table entry. Notice that R2 has a route to the 192.168.6.0/24 network with an AD value of 90.

D 192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0

R2 is running both RIP and EIGRP routing protocols. Remember, it is not common for routers to run multiple dynamic routing protocols, but is used here to demonstrate how administrative distance works. R2 has learned of the 192.168.6.0/24 route from R1 through EIGRP updates and from R3 through RIP updates. RIP has an administrative distance of 120, but EIGRP has a lower administrative distance of 90. So, R2 adds the route learned using EIGRP to the routing table and forwards all packets for the 192.168.6.0/24 network to Router R1.

What happens if the link to R1 becomes unavailable? Would R2 not have a route to 192.168.6.0? Actually, R2 still has RIP route information for 192.168.6.0 stored in the RIP database. This can be verified with the show ip rip database command, as shown in Example 3-3.

Example 3-3  Verifying RIP Route Availability

R2# show ip rip database

192.168.3.0/24    directly connected, FastEthernet0/0
192.168.4.0/24    directly connected, Serial0/0/1
The `show ip rip database` command shows all RIP routes learned by R2, whether or not the RIP route is installed in the routing table. Now you can answer the question as to what would happen if the EIGRP route to 192.168.6.0 became unavailable. RIP has a route, and it would be installed in the routing table. If the EIGRP route is later restored, the RIP route would be removed and the EIGRP route would be reinstalled because it has a better AD value.

### Dynamic Routing Protocols and Administrative Distance

You already know that you can verify AD values with the `show ip route` command, as shown previously in Example 3-2.

Example 3-4 shows that the AD value can also be verified with the `show ip protocols` command. This command displays all pertinent information about routing protocols operating on the router.

#### Example 3-4  Verify Administrative Distance with the `show ip protocols` Command

```plaintext
R2# show ip protocols

Routing Protocol is "eigrp 100"

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100
Automatic network summarization is in effect
```
You will see additional coverage of the `show ip protocols` command many times during the rest of the course. However, for now, notice the highlighted output: R2 has two routing protocols listed, and the AD value is called Distance.

Table 3-2 shows the different administrative distance values for various routing protocols.
### Table 3-2  Default Administrative Distances

<table>
<thead>
<tr>
<th>Route Source</th>
<th>AD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>0</td>
</tr>
<tr>
<td>Static</td>
<td>1</td>
</tr>
<tr>
<td>EIGRP summary route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>Internal EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>IS-IS</td>
<td>115</td>
</tr>
<tr>
<td>RIP</td>
<td>120</td>
</tr>
<tr>
<td>External EIGRP</td>
<td>170</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
</tbody>
</table>

### Static Routes and Administrative Distance

As you know from Chapter 2, static routes are entered by an administrator who wants to manually configure the best path to the destination. For that reason, static routes have a default AD value of 1. This means that after directly connected networks, which have a default AD value of 0, static routes are the most preferred route source.

There are situations when an administrator will configure a static route to the same destination that is learned using a dynamic routing protocol, but using a different path. The static route will be configured with an AD greater than that of the routing protocol. If there is a link failure in the path used by the dynamic routing protocol, the route entered by the routing protocol is removed from the routing table. The static route will then become the only source and will automatically be added to the routing table. This is known as a **floating static route** and is discussed in CCNP courses.

A static route using either a next-hop IP address or an exit interface has a default AD value of 1. However, the AD value is not listed in the `show ip route` output when you configure a static route with the exit interface specified. When a static route is configured with an exit interface, the output shows the network as directly connected through that interface.

Using the topology shown in Figure 3-11 and the `show ip route` command for R2 shown in Example 3-5, you can examine the two types of static routes.
Figure 3-11  Administrative Distances and Static Routes

Example 3-5  Routing Table for R2

R2# show ip route

<output omitted>

Gateway of last resort is not set

    172.16.0.0/24 is subnetted, 3 subnets
          C   172.16.1.0 is directly connected, FastEthernet0/0
          C   172.16.2.0 is directly connected, Serial0/0/0
S     172.16.3.0 is directly connected, Serial0/0/0
          C   192.168.1.0/24 is directly connected, Serial0/0/1
          S   192.168.2.0/24 [1/0] via 192.168.1.1

The static route to 172.16.3.0 is listed as directly connected. However, there is no information on what the AD value is. It is a common misconception to assume that the AD value of this route must be 0 because it states “directly connected.” However, that is a false assumption. The default AD of any static route, including those configured with an exit interface, is 1. Remember, only a directly connected network can have an AD of 0. This can be verified by extending the `show ip route` command with the `[route]` option. Specifying the `[route]` reveals detailed information about the route, including its distance, or AD value.

The `show ip route 172.16.3.0` command in Example 3-6 reveals that, in fact, the administrative distance for static routes—even with the exit interface specified—is 1.
Directly Connected Networks and Administrative Distance

Directly connected networks appear in the routing table as soon as the IP address on the interface is configured and the interface is enabled and operational. The AD value of directly connected networks is 0, meaning that this is the most preferred routing source. There is no better route for a router than having one of its interfaces directly connected to that network. For that reason, the administrative distance of a directly connected network cannot be changed, and no other route source can have an administrative distance of 0.

The output of the `show ip route` command in Example 3-7 highlights the directly connected networks with no information about the AD value.

---

**Example 3-7** Directly Connected Networks in Routing Table Do Not Show AD Value

```
R2# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/24 is subnetted, 3 subnets

C  172.16.1.0 is directly connected, FastEthernet0/0
C  172.16.2.0 is directly connected, Serial0/0/0
S  172.16.3.0 is directly connected, Serial0/0/0
C  192.168.1.0/24 is directly connected, Serial0/0/1
S  192.168.2.0/24 [1/0] via 192.168.1.1
```
The output is similar to the output for static routes that point to an exit interface. The only difference is the letter C at the beginning of the entry, which indicates that this is a directly connected network.

To see the AD value of a static route configured with an exit-interface, use the [route] option, as shown in Example 3-8.

**Example 3-8  AD Value Shown for Static Route Configured with an Exit-Interface**

```
R2# show ip route 172.16.3.0
```

Routing entry for 172.16.1.0/24
Known via “connected”, distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via FastEthernet0/0
  Route metric is 0, traffic share count is 1

The `show ip route 172.16.1.0` command reveals that the distance is 0 for that directly connected route.

**Viewing Routing Table Information—show ip route (3.4.4)**

In this activity, you will use a version of the `show ip route` command to see details of routing table entries. Use file e2-344.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.
Summary

Dynamic routing protocols are used by routers to automatically learn about remote networks from other routers. In this chapter, you were introduced to several different dynamic routing protocols.

You learned the following about routing protocols:

- They can be classified as classful or classless.
- They can be a distance vector, link-state, or path vector type.
- They can be an interior gateway protocol or an exterior gateway protocol.

The differences in these classifications will become better understood as you learn more about these routing concepts and protocols in later chapters.

Routing protocols not only discover remote networks but also have a procedure for maintaining accurate network information. When there is a change in the topology, it is the function of the routing protocol to inform other routers about this change. When there is a change in the network topology, some routing protocols can propagate that information throughout the routing domain faster than other routing protocols.

The process of bringing all routing tables to a state of consistency is called convergence. Convergence is when all the routers in the same routing domain or area have complete and accurate information about the network.

Metrics are used by routing protocols to determine the best path or shortest path to reach a destination network. Different routing protocols can use different metrics. Typically, a lower metric means a better path. Five hops to reach a network is better than ten hops.

Routers sometimes learn about multiple routes to the same network from both static routes and dynamic routing protocols. When a Cisco router learns about a destination network from more than one routing source, it uses the administrative distance value to determine which source to use. Each dynamic routing protocol has a unique administrative value, along with static routes and directly connected networks. The lower the administrative value, the more preferred the route source. A directly connected network is always the preferred source, followed by static routes and then various dynamic routing protocols.

All the classifications and concepts in this chapter will be discussed more thoroughly in the rest of the chapters of this course. At the end of this course, you might want to review this chapter to get a review and overview of this information.
Activities and Labs

The activities and labs available in the companion Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide (ISBN 1-58713-204-4) provide hands-on practice with the following topics introduced in this chapter:

Activity 3-1: Subnetting Scenario 1 (3.5.2)
In this activity, you have been given the network address 192.168.9.0/24 to subnet and provide the IP addressing for the network shown in the topology diagram.

Activity 3-2: Subnetting Scenario 2 (3.5.3)
In this activity, you have been given the network address 172.16.0.0/16 to subnet and provide the IP addressing for the network shown in the topology diagram.

Activity 3-3: Subnetting Scenario 3 (3.5.4)
In this activity, you have been given the network address 192.168.1.0/24 to subnet and provide the IP addressing for the network shown in the topology diagram.

Many of the hands-on labs include Packet Tracer Companion Activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide (ISBN 1-58713-204-4) for hands-on labs that have a Packet Tracer Companion.

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. Answers are listed in the appendix, “Check Your Understanding and Challenge Questions Answer Key.”

1. What are two advantages of static routing over dynamic routing?
   A. The configuration is less error prone.
   B. Static routing is more secure because routers do not advertise routes.
   C. Growing the network usually does not present a problem.
   D. No computing overhead is involved.
   E. The administrator has less work maintaining the configuration.
2. Match the description to the proper routing protocol.

Routing protocols:

RIP
IGRP
OSPF
EIGRP
BGP

Description:
A. Path vector exterior routing protocol:
B. Cisco advanced interior routing protocol:
C. Link-state interior routing protocol:
D. Distance vector interior routing protocol:
E. Cisco distance vector interior routing protocol:

3. Which statement best describes convergence on a network?

A. The amount of time required for routers to share administrative configuration changes, such as password changes, from one end of a network to the other end
B. The time required for the routers in the network to update their routing tables after a topology change has occurred
C. The time required for the routers in one autonomous system to learn routes to destinations in another autonomous system
D. The time required for routers running disparate routing protocols to update their routing tables

4. Which of the following parameters are used to calculate metrics? (Choose two.)

A. Hop count
B. Uptime
C. Bandwidth
D. Convergence time
E. Administrative distance

5. Which routing protocol has the most trustworthy administrative distance by default?

A. EIGRP internal routes
B. IS-IS
C. OSPF
D. RIPv1
E. RIPv2
6. How many equal-cost paths can a dynamic routing protocol use for load balancing by default?
   A. 2
   B. 3
   C. 4
   D. 6

7. Which command will show the administrative distance of routes?
   A. R1# show interfaces
   B. R1# show ip route
   C. R1# show ip interfaces
   D. R1# debug ip routing

8. When do directly connected networks appear in the routing table?
   A. When they are included in a static route
   B. When they are used as an exit interface
   C. As soon as they are addressed and operational at Layer 2
   D. As soon as they are addressed and operational at Layer 3
   E. Always when a no shutdown command is issued

9. Router R1 is using the RIPv2 routing protocol and has discovered multiple unequal paths to reach a destination network. How will Router R1 determine which path is the best path to the destination network?
   A. Lowest metric.
   B. Highest metric.
   C. Lowest administrative distance.
   D. Highest administrative distance.
   E. It will load-balance between up to four paths.

10. Enter the proper administrative distance for each routing protocol.
    A. eBGP:
    B. EIGRP (Internal):
    C. EIGRP (External):
    D. IS-IS:
    E. OSPF:
    F. RIP:
11. Designate the following characteristics as belonging to either a classful routing protocol or a classless routing protocol.

A. Does not support discontiguous networks:
B. EIGRP, OSPF, and BGP:
C. Sends subnet mask in its routing updates:
D. Supports discontiguous networks:
E. RIP version 1 and IGRP:
F. Does not send subnet mask in its routing updates:

12. Explain why static routing might be preferred over dynamic routing.

13. What are four ways of classifying dynamic routing protocols?

14. What are the most common metrics used in IP dynamic routing protocols?

15. What is administrative distance, and why is it important?

Challenge Questions and Activities

These questions require a deeper application of the concepts covered in this chapter and are similar to the style of questions you might see on a CCNA certification exam. You can find the answers to these questions in the appendix, “Answers to Check Your Understanding and Challenge Questions and Activities.”

1. It can be said that every router must have at least one static route. Explain why this statement might be true.

2. Students new to routing sometimes assume that bandwidth is a better metric than hop count. Why might this be a false assumption?

To Learn More

Border Gateway Protocol (BGP) is an inter-autonomous routing protocol—the routing protocol of the Internet. Although BGP is only briefly discussed in this course (it is discussed more fully in CCNP), you might find it interesting to view routing tables of some of the Internet core routers.

Route servers are used to view BGP routes on the Internet. Various websites provide access to these route servers, for example, http://www.traceroute.org. When choosing a route server in a specific autonomous system, you will start a Telnet session on that route server. This server is mirroring an Internet core router, which is most often a Cisco router.
You can then use the `show ip route` command to view the actual routing table of an Internet router. Use the `show ip route` command followed by the public or global network address of your school, for example, `show ip route 207.62.187.0`.

You will not be able to understand much of the information in this output, but these commands should give you a sense of the size of a routing table on a core Internet router.
This page intentionally left blank
accessing devices on directly connected networks, 93-96
ACK packets, EIGRP, 403
address table, populating, 24-25
administrative distance, 165
    of directly connected networks, 172-173
    EIGRP, 407
    OSPF, 507
purpose of, 165-168
RIPv1, 226-227
verifying for dynamic routing protocols, 168-169
    for static routing protocols, 170-171
advantages
    of distance vector routing protocols, 188-189
    of dynamic routing protocols, 152-153
    of static routing protocols, 153
algorithms, 186
ARPANET, 4
AS (autonomous system), 154
    EIGRP, configuring, 412
ASBRs (autonomous system boundary routers), 546-548
asymmetric routing, 43
authentication
    EIGRP, 408
    OSPF, 508
    RIPv2, 328
automatic summarization
    EIGRP, disabling, 448-453
    RIPv1, 238-242
        advantages of, 246
        boundary routers, 242
disadvantages of, 247-248
    verifying, 244-246
    RIPv2, 313-315
disabling, 315-316
AUX port, 18

bandwidth, 47-48, 161
    EIGRP, fine tuning, 460-461
    link-state protocol requirements, 491
bandwidth command, 427-429, 527-529
bandwidth metric (EIGRP), 425
banners, router configuration, 27
BDRs, election process, 505, 536-542
best path determination, 5-6, 46-47, 352, 356-358
bootstrap program, 12
bootup process, 11
    bootstrap program, 12
    POST, 12
    setup mode, 13-14
    startup configuration file, 13
    verifying, 14-17
boundary routers, 242
bounded updates
    EIGRP, 405
    routing table maintenance, 198
BR election process, interface priority, 542-543
broadcast updates, 186
BSD (Berkely Software Distribution), 221
child routes, 346-347
    in classless networks, 348-350
    longest matches, 363-367
CIDR (Classless Inter-Domain Routing), 269, 277, 307-309
    route summarization, 278-279
    supernetting on RIPv2 networks, 321-322
    VLSM, 270
Cisco IOS Software, 10
    configuration files, 11
classful IP addressing, 264-265, 268
    high-order bits, 266
    IPv4 addressing structure, 267-268
classless routing, 158, 188
    effect on lookup process, 371-375
    RIPv1, 225
    subnet mask determination, 304-305
    versus classless routing protocols, 290
classless IP addressing, 269
CIDR, 270-271, 277
    route summarization, 278-279
    parent/child routes, 348-350
classless routing, 159, 188, 271-272
    effect on lookup process, 375-381
CLI (command-line interface), 14
cold start, 190-191
Coltun, Rob, 501
commands
    bandwidth, 427-429, 527-529
debug ip rip, 235-236, 244-246
ip ospf cost, 528-529
ip ospf priority, 542-543
ip route, 105-106
    static routes, configuring, 106-110, 115-117
    static routes, modifying, 117-118
    static routes, verifying configuration, 108, 118-121
network, 229-231, 414-416, 512-513
ping, 326
    route print, 36-37
    route redistribute static, 298

Calculating
    EIGRP composite metric value, 423-425, 429-431
    route summaries, 279-280
    summary routes, 125
CDP (Cisco Discovery Protocol)
    disabling, 104
    Layer 2 neighbors, 100-101
    Layer 3 neighbors, 99
    for network discovery, 103-104
characteristics of RIPv1, 222
router eigrp, 414
router ospf, 512
router ospf process_id, 471
router rip, 228-229
router-id, 516
show cdp neighbors, 101-103
show interfaces, 72-74
show ip interface brief, 33-34, 74, 324
show ip ospf, 512
show ip ospf interface, 228-229
show ip ospf neighbor, 514-517
show ip protocols, 233-234, 324
show ip rip, 228-229
show ip rip database, 167
show ip route, 32-36, 162, 231-233, 324
show protocols, 519
show running-config, 29-31, 76, 327
show version, 14-17

comparing
distance vector protocols and enhanced distance vector protocols, 394-395
dynamic and static routing, 152
hop count and bandwidth metrics, 47-48
link-state protocols, 491-492
routing protocol features, 189

composite metric (EIGRP), calculating, 423-425, 429-431

configuration register, 17

configuring
default static routes, 128
EIGRP, 409-411
autonomous systems, 412
bandwidth, 427-429
default route, 457-460
Hello intervals, 461
manual summarization, 456-457
network command, 414-416
process ID, 413
router eigrp command, 414
verifying configuration, 416-419
OSPF, 508, 510-511
loopback address, 515-516
network command, 512-513
router ID, 514-517
router ospf command, 512
RIPv1, 227-228
automatic summarization, 238-242
default route propagation, 253-254
for discontiguous topology, 248-250
networks, specifying, 229-231
passive interfaces, 236-238
router rip command, 228-229
verifying configuration, 231-236
RIPv2, 309-310
classless routing, 311-312
routers
banner, 27
Ethernet interfaces, 76-79
host name, 25-26
interfaces, 27-28
serial interfaces, 82-85
static routes, 105-107
to remote networks, 108-110
verifying configuration, 108, 118-121
with exit interface, 115-117
summary routes, 126-127

connectivity, verifying for RIPv2, 298-299
console port, 18
dead time, modifying, 550-552
default static routes, 127-128
configuring, 128
verifying configuration, 129-130
delay, 161
device access, 93-96

Dijkstra, E.W., 405, 470
directly connected networks, 34-38, 87, 474-476
accessing devices, 93-96
AD, 172-173
installed routing table routes, 89-90
interface configurations, removing, 91-93
pinging devices, 96, 99
disabling
automatic summarization, 315-316
CDP, 104
EIGRP automatic summarization, 448-453
discontiguous address assignment, 264
discontiguous networks, 291
RIPv, configuring, 248-250
RIPv2 support, 301-304
displaying
interface status, 72-76
routing table contents, 35-36, 88-89
OSPF, 522-523
distance vector protocols, 156-157, 182-184
algorithms, 186
broadcast updates, 186
count-to-infinity, 202
CPU processing requirements, link-state protocols, 491

data link layer, MAC layer frame format, 45-46
DB-60 serial connectors, 69
DBD (database description) packets, 502
dead time, modifying, 550-552
debug ip ip rip command, 235-236, 244-246
default routes, 342
EIGRP, 457-460
OSPF, redistribution, 546-548
RIPv1, 250-254
default static routes, 127-128
configuring, 128
verifying configuration, 129-130
delay, 161
devices
accessing on directly connected networks, 93-96
pinging on directly connected networks, 96, 99

directly connected networks, 34-38, 87, 474-476
accessing devices, 93-96
AD, 172-173
installed routing table routes, 89-90
interface configurations, removing, 91-93
pinging devices, 96, 99
disabling
automatic summarization, 315-316
CDP, 104
EIGRP automatic summarization, 448-453
discontiguous address assignment, 264
discontiguous networks, 291
RIPv, configuring, 248-250
RIPv2 support, 301-304
displaying
interface status, 72-76
routing table contents, 35-36, 88-89
OSPF, 522-523
distance vector protocols, 156-157, 182-184
algorithms, 186
broadcast updates, 186
count-to-infinity, 202
CPU processing requirements, link-state protocols, 491

D
-configuring, 409-416, 427-429
default route, 457-460
DUAL, 405-407, 432-438
FC, 434
FD, 432, 435-438
FS, 434-438
Hello intervals, configuring, 461
Hello protocol, 404
manual summarization, 453-457
message format, 396-399
packets, 402-404
PDMs, 400
RD, 434-435
routing table, 419-422, 447-448
verifying configuration, 416-419
features, comparing, 189
network discovery
cold start, 190-191
convergence, 194
initial routing information
exchange, 191-192
routing information exchange, 192-194
periodic updates, 185
RIP, 210-211, 220
administrative distance, 226-227
automatic summarization, 238-242
automatic summarization, advantages of, 246
automatic summarization, disadvantages of, 247-248
automatic summarization, verifying, 244-246
characteristics of, 222
classful routing, 225
configuring, 227-231
default routes, 250-254
discontiguous networks, configuring, 248-250
evolution of, 221
message format, 222-224
passive interfaces, configuring, 236-238
processing updates, 243-244
Request/Response process, 225
timers, 196
verifying configuration, 231-236
routing loops, 200
implications of, 201-202
preventing, 203-210
routing table maintenance
bounded updates, 198
periodic updates, 195-198
synchronization, 199
triggered updates, 198-199
versus enhanced distance vector protocols, 394-395
Doyle, Jeff, 480
DRothers, 505
DRs (designated routers)
election process, 505, 536-543
multiaccess network management, 534-536
DUAL (Diffusing Update Algorithm), 212, 393, 405, 432
FC, 434
FD, 432, 435-438
FS, 434-440
FSM, 407, 440-446
RD, 434-435
successors, 432, 435-438
default route, 457-460
DUAL, 405-407, 432-438
FC, 434
FD, 432, 435-438
FS, 434-440
FDM, 407, 440-446
RD, 434-435
successors, 432, 435-438
default route, 457-460
DUAL, 405-407, 432-438
FC, 434
FD, 432, 435-438
FS, 434-440
FDM, 407, 440-446
RD, 434-435
successors, 432, 435-438
Hello intervals, configuring, 461
Hello protocol, 404
hold time, 397
manual summarization, 453-457
message format, 396-399
metrics
bandwidth, 425
load, 427
reliability, 427
packets, 402-404
PDMs, 400
process ID, configuring, 413
routing table, 419-422
Null0 summary route, 421-422, 447-448
routing table maintenance, bounded updates, 198
verifying configuration, 416-419
election process, DDr/BDRs, 536-542
enhanced distance vector protocols
EIGRP. See EIGRP
versus traditional distance vector protocols, 394-395
equal-cost load balancing, 48, 164-165
versus unequal-cost load balancing, 49
Ethernet
connectors, 70-71
interfaces
configuring, 76-79
static routes, 121-123
verifying configuration, 80-81
event-driven updates, 488
evolution
of dynamic routing protocols, 149 of RIPv1, 221
External Routes TLV, 400

EGPs (exterior gateway protocols), 154-156
EIGRP (Enhanced IGRP), 210-211, 393
AD, 407
authentication, 408
automatic summarization, disabling, 448-453
autonomous systems, configuring, 412
bandwidth utilization, fine tuning, 460-461
bounded updates, 405
composite metric value, 423-425, 429-431
configuration commands, 414-416, 427-429
classful routing, configuring, 227-231
discontiguous networks, configuring, 248-250
evolution of dynamic routing protocols, 149 of RIPv1, 221
EIGRP. See EIGRP
equal-cost load balancing, 48, 164-165
versus unequal-cost load balancing, 49
Ethernet
event-driven updates, 488
evolution
equal-cost load balancing, 48, 164-165
versus unequal-cost load balancing, 49
Ethernet
FC (feasibility condition), 434
FD (feasible distance), 432, 438
Ferguson, Dennis, 501
fields
of IP packets, 44-45
of OSPF Hello packets, 503
firmware, 9
five-in-one serial ports, 68
flapping links, 521
flash memory, 10
floating static routes, 170
flooding LSAs, 533-534
flush timers, 196
frames, MAC Layer format, 45-46
FS (feasible successors), 434-440
FSM (Finite State Machine), 440, 446
Garcia-Luna-Aceves, J.J., 405
GATED, 501
general operations of dynamic routing protocols, 151
GWINFO (Gateway Information Protocol), 221
Hedrick, Charles, 221
Hello interval (EIGRP), configuring, 461
Hello packets
EIGRP, 402
OSPF, 502
Hello protocol
EIGRP, 404
OSPF
Dead interval, 505
neighbor establishment, 504
high-order bits, 266
history of OSPF, 500
hold-down timers, 196, 395
routing loops, preventing, 203-205
hold time, 397
hop count, 47-48, 155, 161
host name, router configuration, 25-26
hybrid routing protocols, EIGRP. See EIGRP
IGPs (Interior Gateway Protocol), 154-156
distance vector protocols, 156-157
link-state protocols, 157
IMP (Interface Message Processor), 4 initial routing information exchange, 191-192
interfaces, 4, 18
directly connected networks, 34, 37-38
Ethernet
configuring, 76-79
static routes, 121-123
verifying configuration, 80-81
example of, 20-21
LAN interfaces, 20
LED status indicators, 19
router configuration, 27-28
serial interfaces
configuring, 82-85
verifying configuration, 85-87
status of, displaying, 72-76
Internal Routes TLV, 398
invalid timers (RIP), 196
IOS. See Cisco IOS Software
IP addressing
classful, 265, 268
high-order bits, 266
IPv4 addressing structure,
267-268
classless, 269
CIDR, 270-271, 277-279
subnetting, VLSM, 272, 275-276
ip ospf cost command, 528-529
ip ospf priority command, 542-543
IP packet fields, 44-45
ip route command, 105-106
configuring static routes, 106-110, 115-117
modifying static routes, 117-118
verifying static route configuration, 108, 118-121
IP routing protocols, 41-42
IS-IS (Intermediate System-to-Intermediate System), comparing with OSPF, 491-492
ISC (Internet Software Consortium), 265
ISPs (Internet Service Providers), 415, 416
IS-IS (Intermediate System-to-Intermediate system), comparing with OSPF, 491-492
level 1 routes, 341-342
longest matches, 358-359
parent routes, 344-346
in classless networks, 348-350
longest matches, 363-367
ultimate routes, longest matches, 359-362
level 2 routes, 345
child routes, 346-347
in classless networks, 348-350
longest matches, 363-367
limitations of RIPv1, 291
link-state database, building, 480-482
link-state protocols, 157, 470
advantages of, 488
corevance speed, 488
event-driven updates, 488
hierarchical design, 489
comparing, 491-492
requirements, 489, 491
routing process, 474
directly connected networks, discovering, 474-476
link-state database, building, 480-482
LSP flooding, 479-480
LSP generation, 478
neighbor discovery, 477
SPF algorithm, 471-473
SPF tree
building, 482-487
routing table, generating, 487
link states, 476
links, 475
load, 161
load balancing, 163
load metric (EIGRP), 427
longest matches, 358-367
lookup process, 350-351
best path determination, 352, 356-358
longest matches, 358-367
routing behavior effect on, 368-370
classful behavior, 371-375
classless behavior, 375-381
VLSM effect on, 367
loopback address (OSPF), configuring, 515-516
loopback interfaces, 297
LSAck (link-state acknowledgment), 502
LSAs (link-state advertisements), 502
flooding, 533-534
LSPs (link-state packets), 474
flooding to neighbors, 479-480
generating on link-state protocols, 478
LSRs (link-state requests), 502
LSUs (link-state updates), 502, 505

MAC layer frame format, 45-46
management ports, 18
manual summarization, EIGRP, 453-457
memory
flash memory, 10
link-state protocol requirements, 491
NVRAM, 10
RAM, 9
ROM, 9
messages
EIGRP, 396-399
OSPF, encapsulation, 501
RIPv1, 222-224
metrics, 160-162
bandwidth, 47-48
cost, 523-524
modifying, 527-529
reference bandwidth, 524, 548-550
verifying, 526
EIGRP
bandwidth, 425
load, 427
reliability, 427
hop count, 47-48, 155
routing loops, preventing, 203
missing routes, troubleshooting, 132-134
modifying
Dead time, 550-552
OSPF cost, 527-529
OSPF interface priority, 543
OSPF router ID, 516
duplicates, troubleshooting, 517
reference bandwidth, 549-550
static routes, 117-118
MOTD banners, router configuration, 27
Moy, John, 501
multiaccess networks, 530-531
DRs, 534, 536
LSAs, flooding, 533-534
multiple adjacencies, 531-532
OSPF
DR/BDR election process, 536-542
interface priority, 542-543
multiarea OSPF, configuring, 513

neighbor discovery, link-state protocols, 477
neighbor relationships (OSPF)
adjacencies, verifying, 553
establishing, 504
verifying, 517
neighbors, 186
network command, 229-231, 414-416, 512-513
network discovery, 41
CDP, 99-104
cold start, 190-191
convergence, 194
initial routing information exchange, 191-192
routing information exchange, 192-194
network layer (OSI model), routing, 21-22
network routes, 342
next hop, 34
NICs (network interface cards), 20
null interfaces, 298
Null0 summary route (EIGRP), 421-422, 447-448
NVRAM (non-volatile RAM), 10

OSPF
AD, 507
authentication, 508
bandwidth value, 525-527
BDR election process, 505, 536-542
comparing with IS-IS, 491-492
configuring, 508-513
cost metric, 523-524
modifying, 527-529
reference bandwidth, 524
verifying, 526
Dead intervals, troubleshooting, 521
Dead time, modifying, 550-552
default route redistribution, 546-548
DR election process, 505, 536-542
flapping links, 521
Hello protocol
Dead interval, 505
neighbor establishment, 504
history of, 500
loopback address, configuring, 515-516
message encapsulation, 501
multiaccess networks, 530-531
DRs, 534-536
interface priority, 542-543
LSAs, flooding, 533-534
multiple adjacencies, 531-532
neighbor relationships, verifying, 518
adjacencies, 553
packets, 502
Hello, 502
LSUs, 505
reference bandwidth, 548
modifying, 549-550
router ID, 514
duplicates, troubleshooting, 517
modifying, 516
verifying, 514-515
routing table
displaying, 522-523
populating, 506
troubleshooting, 518-521

P-Q
packets
EIGRP, 401-404
bounded updates, 405
fields, 396-397, 399
hello, 404
forwarding, 130-132
IP, fields, 44-45
OSPF, 502
Hello, 502
LSUs, 505
parent routes, 344, 346
in classless networks, 348-350
longest matches, 363-367
passive interfaces, configuring on RIPv1, 236-238
path determination, 50-51
comparing traditional distance vector protocols and enhanced distance vector protocols, 395
path vector protocols, 156
PDMs (protocol-dependent modules), 400
periodic updates, 185, 195-198
ping command, 326
pinging devices on directly connected networks, 96, 99
point-to-point networks, 530
static routes, 117
poison reverse, preventing routing loops, 208-209
populating address table, 24-25
ports, management ports, 18
POST (power-on self test), 12
preventing routing loops
via hold-down timers, 203-205
via maximum metric value, 203
via split horizon, 206-209
via TTL, 209-210
principles of static routes, 110-111
applying, 111-113
private addressing, RFC 1918, 295
privileged EXEC mode, 25
process ID (EIGRP), configuring, 413
processing RIPv1 processing, 243-244
purpose of dynamic routing protocols, 151

R

RAM, 9
RD, 434-435
recursive route lookups, 113-115
redistribute static command, 298
redistribution, 295
reference bandwidth, 524, 548
modifying, 549-550
reliability, 161
reliability metric (EIGRP), 427
remote networks, 35
removing directly connected networks from routers, 91-93
Request/Response process, RIPv1, 225
requirements for link-state routing protocols, 489-491
resource usage, 188
RFC 1918, 295
RIP, 210-211. See also RIPv1; RIPv2
hop count, 155
routing table maintenance, 196-198
triggered updates, 198-199
timers, 196
RIPv1, 220
administrative distance, 226-227
automatic summarization, 238-242
advantages of, 246
boundary routers, 242
disadvantages of, 247-248
verifying, 244-246
characteristics of, 222
classful routing, 225
configuring, 227-231
default routes, 250-254
discontiguous networks, configuring, 248-250
evolution of, 221
limitation of, 291
message format, 222-224
passive interfaces, configuring, 236-238
Request/Response process, 225
subnetting, 305-309
topology limitations, 297
updates, processing, 243-244
verifying configuration, 231-236
RIPv2, 290-291
addressing table, 291
authentication, 328
auto summarization, disabling, 315-316
CIDR, 321-322
classless routing, configuring, 311-312
configuring, 309-310
connectivity, verifying, 298-299
discontiguous network support, 301-304
discontiguous networks, 291
route summarization, 313-315
summary routes, 295
troubleshooting, 328
troubleshooting commands, 323-327
update message, verifying, 316-319
VLSM, 295, 320
RIP_JITTER variable (update interval), 199
role of dynamic routing protocols, 150
ROM, 9
route poisoning, 207
route print command, 36-37
route redistribution, 298
route resolvability, 113-115
route summarization, 278-280
EIGRP
automatic summarization, disabling, 448-453
manual summarization, 453-457
RIPv1, 238-242
boundary routers, 242
RIPv2, 313-315
static route summarization, 124-127
router eigrp command, 414
router ID (OSPF), 514
duplicates, troubleshooting, 517
modifying, 516
verifying, 514-515
router-id command, 516
router ospf command, 512
router ospf process-id command, 471
router rip command, 228-229
routers
address table, populating, 24-25
banners, configuring, 27
best path determination, 5-6, 46-47
bootup process, 11
bootstrap program, 12
POST, 12
setup mode, 13-14
startup configuration file, 13
verifying, 14-17
CLI, 14
connectors, 68
    Ethernet connectors, 70-71
    serial connectors, 68
CPU, 9
directly connected networks, 87
devices, accessing, 93-96
devices, pinging, 96, 99
installed routing table routes, 89-90
interface configurations, removing, 91-93
Ethernet interfaces
    configuring, 76-79
    verifying configuration, 80-81
flash memory, 10
interfaces, 4, 18
    configuring, 27-28
    directly connected networks, 37-38
    example, 20-21
LAN interfaces, 20
status indicators, 19
status of, displaying, 72-76
Layer 1 operation, 23
Layer 2 operation, 23
Layer 3 operation, 21-22
management ports, 18
naming, 25-26
NVRAM, 10
path determination, 50-51
RAM, 9
ROM, 9
serial interfaces
    configuring, 82-85
    verifying configuration, 85-87
services provided, 3
switching function, 51-57
user mode, 25
verifying configuration, 29-34
routing behaviors, effect on lookup process, 368-370
    classful routing, 371-375
    classless routing, 375-381
routing domains. See AS (autonomous system)
routing information exchange, 192-194
routing loops, 200
    implications of, 201-202
    preventing
        via hold-down timers, 203-205
        via maximum metric value, 203
via split horizon, 206-209
via TTL, 209-210
routing process for link-state protocols, 474
directly connected networks, discovering, 474-476
link-state database, building, 480-482
LSP flooding, 479-480
LSP generation, 478
neighbor discovery, 477
routing protocols, advantages/disadvantages of, 188-189
routing table, 79, 88-89
    basic principles, 42-43
    best path determination, 5
    directly connected networks, 89-90
        interface configurations, removing, 91-93
    displaying, 35-36
    dynamic routing, 40-41
    IP routing protocols, 41-42
    EIGRP, 419-422
        Null0 summary route, 421-422, 447-448
    entry information, maintaining, 340
        bounded updates, 198
        periodic updates, 195-198
        synchronization, 199
        triggered updates, 198-199
    generating from SPF tree, 487
    level 1 routes, 341-342
    parent routes, 344-346
    level 2 routes, 345
    child routes, 346-347
    lookup process, 350-351
        best path determination, 352, 356-358
        classful routing behavior effect on, 371-375
        classless routing behavior effect on, 375-376, 379-381
    longest matches, 358-367
    routing behavior effect on, 368-370
    VLSM effect on, 367
    next hop, 34
    OSPF
        displaying, 522-523
        populating, 506
    static routes
        principles, 110-113
        route resolvability, 113-115
        when to use, 39-40
    structure, 338
RTP (Real-Time Transport Protocol), 392
RTP (Reliable Transport Protocol), 401
scalability, 188
Scholten, C.S., 405
serial connectors, 68
serial interfaces
    configuring, 82-83
    cost metric, modifying, 527-529
    CSU/DSU connection, configuring, 83
    default bandwidth, 525-527
    for lab environment, configuring, 84-85
    verifying configuration, 85-87
setup mode, 13-14
show cdp neighbors command, 101-103
show interfaces command, 72-74
show ip interface brief command, 33-34, 74, 324
show ip ospf command, 520-521
show ip ospf interface, 552
show ip ospf interface command, 521
show ip ospf neighbor command, 518-519, 550-551
show ip protocols command, 233-234, 324, 519
show ip rip command, 325-326
show ip rip database command, 167
show ip route command, 32-36, 162, 231-233, 323
show running-config command, 29-31, 76, 327
show version command, 14-17
single-area OSPF, 513
smart serial interfaces, 69
SPF algorithm, 470-473
SPF schedule delay, 521
SPF tree
building, 482-487
routing table, generating, 487
split horizon
routing loops, preventing, 206-209
with poison reverse, 208-209
startup configuration file, 13
static routes, 35, 39, 298
administrative distance, verifying, 170-171
advantages of, 153
configuring, 105-107
default static routes, 127-128
configuring, 128
verifying configuration, 129-130
floating static routes, 170
metrics, 162
modifying, 117-118
and packet forwarding, 130-132
principles, 110-111
applying, 111-113
to remote networks, configuring, 108-110
route resolvability, 113-115
summary static routes, 124-125
configuring, 126-127
verifying configuration, 108, 118-121
when to use, 39-40
with Ethernet interfaces, 121-123
with exit interface, configuring, 115-117
structure of routing table, 338
classless networks, parent/child routes, 348-350
entries, 340
level 1 routes, 341-342
parent routes, 344-346
level 2 routes, 345
child routes, 346-347
stub networks, 105
stub routers, 105
subnet masks, determining on classful networks, 304-305
subnetting
on RIPv1 networks, 305-309
VLSM, 272, 275-276, 320
successors, 432, 435-438
summary static routes, 124-125
configuring, 126-127
supernet routes, 342

supernetting, 264, 271
RIPv2, CIDR, 321-322
switching function of routers, 51-57
synchronization, routing table maintenance, 199

time to convergence, 188
timers, RIP, 196
TLV (Type/Length/Value) field, 396
External Routes TLV, 400
Internal Routes TLV, 398
topology table, 211
triggered updates, routing table maintenance, 198-199
troubleshooting
missing routes, 132-134
OSPF, 518-521
RIPv2, 323-328
trustworthiness, 166
TTL (Time To Live) values, 200
routing loops, preventing, 209-210

ultimate routes, 342
longest matches, 359-362
unequal-cost load balancing, 49
unified communications, 7
update interval, RIP_JITTER variable, 199
updates
EIGRP, 403
bounded updates, 405
event-driven, 488
RIPv1 processing, 243-244
RIPv2, verifying, 316-319
user mode, 25

verifying
administrative distance
for dynamic routing protocols, 168-169
for static routing protocols, 170-171

W-X-Y-Z

WANs, 5
XNS (Xerox Network System), 221
Zinin, Alex, 110