

#### Official Cert Guide

Learn, prepare, and practice for exam success



## Cisco CCNA

Routing and Switching ICND2 200-101

Academic Edition

ciscopress.com

WENDELL ODOM, CCIE® No. 1624

FREE SAMPLE CHAPTER











In addition to the wealth of updated content, this new edition includes a series of free hands-on exercises to help you master several real-world configuration and trouble-shooting activities. These exercises can be performed on the CCNA ICND2 200-101 Network Simulator Lite software included for free on the DVD that accompanies this book. This software, which simulates the experience of working on actual Cisco routers and switches, contains the following 13 free lab exercises:

- 1. EIGRP Serial Configuration I Skill Builder Lab
- 2. EIGRP Serial Configuration II Skill Builder Lab
- 3. EIGRP Serial Configuration III Skill Builder Lab
- 4. EIGRP Frame Relay Configuration I Skill Builder Lab
- 5. EIGRP Frame Relay Configuration II Skill Builder Lab
- 6. EIGRP Route Tuning I Skill Builder Lab
- 7. EIGRP Route Tuning II Skill Builder Lab
- 8. EIGRP Neighbors II Skill Builder Lab
- 9. EIGRP Neighbors III Skill Builder Lab
- 10. EIGRP Configuration I Configuration Scenario
- 11. EIGRP Configuration II Configuration Scenario
- 12. EIGRP Metric Manipulation Configuration Scenario
- 13. Path Troubleshooting IV Troubleshooting Scenario

If you are interested in exploring more hands-on labs and practicing configuration and troubleshooting with more router and switch commands, check out our full simulator product offerings at http://www.pearsonitcertification.com/networksimulator.

#### CCNA ICND2 200-101 Network Simulator Lite minimum system requirements:

- Microsoft Windows XP (SP3), Windows Vista (32-bit/64-bit) with SP1, Windows 7 (32-bit/64-bit) or Windows 8 (32-bit/64-bit, x86 processors), Mac OS X 10.6, 10.7, or 10.8
- Intel Pentium III 1GHz or faster processor
- 512 MB RAM (1GB recommended)
- 1 GB hard disk space
- 32-bit color depth at 1024x768 resolution
- Adobe Acrobat Reader version 8 and above

#### Other applications installed during installation:

- Adobe AIR 3.6.0
- Captive JRE 6

Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Academic Edition is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/go/authorizedtraining.

# Cisco CCNA

# Routing and Switching ICND2 200-101 Official Cert Guide

**Academic Edition** 

WENDELL ODOM, CCIE No. 1624

**Cisco Press** 

800 East 96th Street Indianapolis, IN 46240

#### **Cisco CCNA Routing and Switching ICND2 200-101**

Official Cert Guide, Academic Edition

Wendell Odom, CCIE No. 1624

Copyright© 2013 Pearson Education, 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

Third Printing: September 2014 with corrections March 2015

Library of Congress Control Number: 2013939885

ISBN-13: 978-1-58714-488-2 ISBN-10: 1-58714-488-3

#### **Warning and Disclaimer**

This book provides information about the Cisco 200-101 ICND2 and 200-120 CCNA exams. 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 corpsales@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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press:

Jan Cornelssen

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Andrew Cupp

Senior Project Editor: Tonya Simpson

Copy Editor: Keith Cline

Technical Editor: Elan Beer

Editorial Assistant: Vanessa Evans

Cover Designer: Mark Shirar

Illustrator: Michael Tanamachi

Composition: Bronkella Publishing

Indexer: Erika Millen

Proofreader: Sarah Kearns



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT. Cisco Eos, Cisco Health-Presence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Stadium/Vision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way New Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aronet, AsyncOS, Bringing the Meeting To You, Catalyst, CDDA, CDDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco Distry, Cisco Systems, Cisco Systems (Sico Systems, Cisco Systems, Link Systems, and Cast Cisco Systems, Cisco Systems, Link Systems, and Cast Cisco Systems, Link Systems, and Cast Cisco Systems, Link Systems, Lin

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company, (0812R)

#### **About the Author**

Wendell Odom, CCIE No. 1624, has been in the networking industry since 1981. He has worked as a network engineer, consultant, systems engineer, instructor, and course developer; he currently works writing and creating certification tools. He is the author of all the previous books in the Cisco Press CCNA Official Certification Guide series, as well as author of the CCNP ROUTE 642-902 Official Certification Guide, the QoS 642-642 Exam Certification Guide, and co-author of the CCIE Routing and Switch Official Certification Guide and several other titles. He is also a consultant for the CCNA 640-802 Network Simulator from Pearson and for a forthcoming replacement version of that product. He maintains study tools, links to his blogs, and other resources at http://www.certskills.com.

#### **About the Contributing Author**

Anthony Sequeira, CCIE No. 15626, is a Cisco Certified Systems Instructor (CCSI) and author regarding all levels and tracks of Cisco certification. Anthony formally began his career in the information technology industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion: teaching and writing about Microsoft and Cisco technologies. Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company KnowledgeNet, and Anthony trained there for many years. Anthony is currently pursuing his second CCIE in the area of Security and is a full-time instructor for the next generation of KnowledgeNet, StormWind Live. Anthony is also a VMware Certified Professional.

#### **About the Technical Reviewer**

Elan Beer, CCIE No. 1837, is a senior consultant and Cisco instructor specializing in data center architecture and multiprotocol network design. For the past 25 years, Elan has designed networks and trained thousands of industry experts in data center architecture, routing, and switching. Elan has been instrumental in large-scale professional service efforts designing and troubleshooting internetworks, performing data center and network audits, and assisting clients with their short- and long-term design objectives. Elan has a global perspective of network architectures via his international clientele. Elan has used his expertise to design and trouble-shoot data centers and internetworks in Malaysia, North America, Europe, Australia, Africa, China, and the Middle East. Most recently, Elan has been focused on data center design, configuration, and troubleshooting as well as service provider technologies. In 1993, Elan was among the first to obtain Cisco's Certified System Instructor (CCSI) certification, and in 1996, he was among the first to attain Cisco System's highest technical certification, the Cisco Certified Internetworking Expert. Since then, Elan has been involved in numerous large-scale data center and telecommunications networking projects worldwide.

#### **Dedication**

In memory of Carcel Lanier (C.L.) Odom: Dad's Pop, Poppa, wearing khakis, quiet, tearing down the old house (one board at a time), tagging along at the cow sales barn, walking the property, and napping during the Sunday morning sermon.

#### **Acknowledgments**

Although published as a first edition for various reasons, this book (and the companion *Cisco CCENT/CCNA ICND1 100-101 Exam Cert Guide*, Academic Edition) represents the seventh book in a long line of Cisco Press books focused on helping people pass the CCENT and CCNA R/S certifications. Given the long history, many people have worked on these books from their inception back in 1998. To those many people who have touched these books over these past 15 years—technical edits, development, copy edits, project editing, proofing, indexing, managing the production process, interior design, cover design, marketing, and all the other details that happen to get these books out the door—thanks so much for playing a role in this CCENT/CCNA franchise.

Many of the contributors to the previous editions returned to work on creating these new editions, including Development Editor Drew Cupp. Drew kept all the details straight, with my frequent changes to the outlines and titles, keeping the sequencing on track, while still doing his primary job: keeping the text and features clear and consistent throughout the book. Thanks, Drew, for walking me through the development.

Contributing author Anthony Sequeira did a nice job stepping in on the network management part of the book. Anthony was a perfect fit, given his interest in management protocols and tools, and his writing experience and his great teaching skills (with enthusiasm!). Thanks for helping make this book complete and doing such a great job.

As for technical editors, Elan Beer did his normal job. That is, he did his usual amazing job of doing every part of the technical edit job well, from finding the tiny little cross-reference errors that lie pages apart, to anticipating how readers might misunderstand certain phrasing, to being all over the details of every technical feature. Fantastic job as usual; thanks, Elan.

Brett Bartow again served as executive editor of the book, as he has almost since the beginning of these titles. When my family has asked me over the years about Brett's role with these books, the best single word definition is *teammate*. Brett may be employed at Pearson Education, but he is always working with me and for me, watching out for the business end of the books and finding ways to make the publisher/author relationship work seamlessly. Thanks for another great ride through these books, Brett!

Word docs go in, and out come these beautiful finished products. Thanks to Sandra Schroeder, Tonya Simpson, and all the production team for working through the magic that takes those Word docs and makes the beautiful finished product. From fixing all my grammar, crummy word choices, passive-voice sentences, and then pulling the design and layout together, they do it all. Thanks for putting it all together and making it look easy. And Tonya, managing the details through several process steps for roughly 100 elements between the pair of CCNA books in a short timeframe: Wow, thanks for the amazing juggling act! And thanks especially for the attention to detail.

The figures for these books go through a little different process than they do for other books. Together we invested a large amount of labor in updating the figures for these books, both for the design, the number of figures, and for the color versions of the figures for the electronic versions of the books. A special thanks goes out to Laura Robbins for working with me on the color and design standards early in the process. Also, thanks to Mike Tanamachi for drawing all the figures so well (and then redrawing them every time I changed my mind about something).

Thanks to Chris Burns of CertSkills for all the work on the mind maps, both those used in the final product and those used to build the book, as well as for being a bit of a test case for some of the chapters.

A special thank you to you readers who write in with suggestions, possible errors, and especially those of you who post online at the Cisco Learning Network. Without question, the comments I receive directly and overhear by participating at CLN made this edition a better book.

Thanks to my wife, Kris. Book schedules have a bigger impact than I would like, but you always make it work. Thanks to my daughter, Hannah, for all the great study/work breaks on some of these busy schooldays. And thanks to Jesus Christ, for this opportunity to write.

#### **Contents at a Glance**

Introduction xxvi
Getting Started 3

#### Part I: LAN Switching 9

Chapter 1: Spanning Tree Protocol Concepts 10

Chapter 2: Spanning Tree Protocol Implementation 36

Chapter 3: Troubleshooting LAN Switching 64

Part I Review 104

#### Part II: IP Version 4 Routing 109

Chapter 4: Troubleshooting IPv4 Routing Part I 110
Chapter 5: Troubleshooting IPv4 Routing Part II 132

Chapter 6: Creating Redundant First-Hop Routers 156

Chapter 7: Virtual Private Networks 176

Part II Review 194

#### Part III: IP Version 4 Routing Protocols 199

Chapter 8: Implementing OSPF for IPv4 200

Chapter 9: Understanding EIGRP Concepts 230

Chapter 10: Implementing EIGRP for IPv4 252

Chapter 11: Troubleshooting IPv4 Routing Protocols 278

Part III Review 304

#### Part IV: Wide Area Networks 309

Chapter 12: Implementing Point-to-Point WANs 310

Chapter 13: Understanding Frame Relay Concepts 336

Chapter 14: Implementing Frame Relay 352

Chapter 15: Identifying Other Types of WANs 386

Part IV Review 404

#### Part V: IP Version 6 409

Chapter 16: Troubleshooting IPv6 Routing 410

Chapter 17: Implementing OSPF for IPv6 434

Chapter 18: Implementing EIGRP for IPv6 460

Part V Review 480

#### x Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Academic Edition

#### Part VI: Network Management 485

Chapter 19: Managing Network Devices 486

Chapter 20: Managing IOS Files 504

Chapter 21: Managing IOS Licensing 526

Part VI Review 542

#### Part VII: Final Review 545

Chapter 22: Final Review 546

#### Part VIII: Appendixes 561

Appendix A: Numeric Reference Tables 563

Appendix B: ICND2 Exam Updates 571

Glossary 598

Index 618

#### **DVD** Appendixes

Appendix C Answers to the Review Questions

Appendix D Memory Tables

Appendix E Memory Tables Answer Key

Appendix F Mind Map Solutions

Appendix G Study Planner

#### **Contents**

Introduction xxvi
Getting Started 3

#### Part I: LAN Switching 9

#### Chapter 1 Spanning Tree Protocol Concepts 10

Foundation Topics 11

LAN Switching Review 11

LAN Switch Forwarding Logic 11

Switch Verification 12

Viewing the MAC Address Table 12

Determining the VLAN of a Frame 13

Verifying Trunks 15

Spanning Tree Protocol (IEEE 802.1D) 15

The Need for Spanning Tree 16

What IEEE 802.1D Spanning Tree Does 18

How Spanning Tree Works 19

The STP Bridge ID and Hello BPDU 20

Electing the Root Switch 21

Choosing Each Switch's Root Port 23

Choosing the Designated Port on Each LAN Segment 24

Influencing and Changing the STP Topology 25

Making Configuration Changes to Influence the STP Topology 25

Reacting to State Changes That Affect the STP Topology 26

How Switches React to Changes with STP 26

Changing Interface States with STP 28

Optional STP Features 29

EtherChannel 29

PortFast 30

BPDU Guard 30

Rapid STP (IEEE 802.1w) 31

Review Activities 32

#### Chapter 2 Spanning Tree Protocol Implementation 36

Foundation Topics 37

STP Configuration and Verification 37

Setting the STP Mode 37

Connecting STP Concepts to STP Configuration Options 38

Per-VLAN Configuration Settings 38

The Bridge ID and System ID Extension 39

Per-VLAN Port Costs 40

STP Configuration Option Summary 40

Verifying STP Operation 40

Configuring STP Port Costs 43

Configuring Priority to Influence the Root Election 45

Configuring PortFast and BPDU Guard 46

Configuring EtherChannel 47

Configuring a Manual EtherChannel 48

Configuring Dynamic EtherChannels 50

STP Troubleshooting 50

Determining the Root Switch 51

Determining the Root Port on Nonroot Switches 52

STP Tiebreakers When Choosing the Root Port 53

Suggestions for Attacking Root Port Problems on the Exam 54

Determining the Designated Port on Each LAN Segment 54

Suggestions for Attacking Designated Port Problems on the Exam 55

STP Convergence 56

Troubleshooting EtherChannel 56

Incorrect Options on the channel-group Command 57

Configuration Checks Before Adding Interfaces to EtherChannels 58

Review Activities 60

#### Chapter 3 Troubleshooting LAN Switching 64

Foundation Topics 65

Generalized Troubleshooting Methodologies 65

Analyzing and Predicting Normal Network Operation 65

Data Plane Analysis 66

Control Plane Analysis 67

Predicting Normal Operations: Summary of the Process 68

Problem Isolation 68

Root Cause Analysis 69

Real World Versus the Exams 70

Troubleshooting the LAN Switching Data Plane 70

An Overview of the Normal LAN Switch Forwarding Process 71

Step 1: Confirm the Network Diagrams Using CDP 72

Step 2: Isolate Interface Problems 73

Interface Status Codes and Reasons for Nonworking States 74

The notconnect State and Cabling Pinouts 75

Determining Switch Interface Speed and Duplex 76

Issues Related to Speed and Duplex 77

Step 3: Isolate Filtering and Port Security Problems 79

	Step 4: Isolate VLAN and Trunking Problems 82
	Ensuring That the Right Access Interfaces Are in the Right VLANs 83
	Access VLANs Not Being Defined or Not Being Active 83
	Identify Trunks and VLANs Forwarded on Those Trunks 84
	Troubleshooting Examples and Exercises 86
	Troubleshooting Example 1: Find Existing LAN Data Plane Problems 86
	Step 1: Verify the Accuracy of the Diagram Using CDP 87
	Step 2: Check for Interface Problems 88
	Step 3: Check for Port Security Problems 90
	Step 4: Check for VLAN and VLAN Trunk Problems 91
	Troubleshooting Example 2: Predicting LAN Data Plane Behavior 94
	PC1 ARP Request (Broadcast) 95
	R1 ARP Reply (Unicast) 98
	Review Activities 102
Part I Revie	w 104
Part II: IP	Version 4 Routing 109
Chapter 4	Troubleshooting IPv4 Routing Part I 110
	Foundation Topics 111
	Predicting Normal IPv4 Routing Behavior 111
	Host IPv4 Routing Logic 111
	Routing Logic Used by IPv4 Routers 112
	IP Routing Logic on a Single Router 112
	IP Routing from Host to Host 113
	Building New Data Link Headers Using ARP Information 114
	Problem Isolation Using the ping Command 115
	Ping Command Basics 115
	Strategies and Results When Testing with the ping Command 116
	Testing Longer Routes from Near the Source of the Problem 117
	Using Extended Ping to Test the Reverse Route 119
	Testing LAN Neighbors with Standard Ping 121
	Testing LAN Neighbors with Extended Ping 122
	Testing WAN Neighbors with Standard Ping 122
	Using Ping with Names and with IP Addresses 123
	Problem Isolation Using the traceroute Command 124
	traceroute Basics 124
	How the traceroute Command Works 125
	Standard and Extended traceroute 126
	Using traceroute to Isolate the Problem to Two Routers 127
	Review Activities 130

#### Chapter 5 Troubleshooting IPv4 Routing Part II 132

Foundation Topics 133

Problems Between the Host and the Default Router 133

Root Causes Based on a Host's IPv4 Settings 133

Ensure IPv4 Settings Correctly Match 133

Mismatched Masks Impact Route to Reach Subnet 134

Typical Root Causes of DNS Problems 136

Wrong Default Router IP Address Setting 137

Root Causes Based on the Default Router's Configuration 137

Mismatched VLAN Trunking Configuration with Router on a Stick 138

DHCP Relay Issues 140

Router LAN Interface and LAN Issues 141

Problems with Routing Packets Between Routers 143

IP Forwarding by Matching the Most Specific Route 143

Using show ip route and Subnet Math to Find the Best Route 144

Using show ip route address to Find the Best Route 145

show ip route Reference 145

Routing Problems Caused by Incorrect Addressing Plans 146

Recognizing When VLSM Is Used or Not 147

Overlaps When Not Using VLSM 147

Overlaps When Using VLSM 148

Configuring Overlapping VLSM Subnets 149

Router WAN Interface Status 150

Filtering Packets with Access Lists 151

Review Activities 153

#### Chapter 6 Creating Redundant First-Hop Routers 156

Foundation Topics 157

FHRP Concepts 157

The Need for Redundancy in Networks 157

The Need for a First Hop Redundancy Protocol 159

The Three Solutions for First-Hop Redundancy 160

HSRP Concepts 160

HSRP Failover 161

HSRP Load Balancing 162

GLBP Concepts 163

FHRP Configuration and Verification 164

Configuring and Verifying HSRP 164

Configuring and Verifying GLBP 167

Review Activities 170

#### Chapter 7 Virtual Private Networks 176

Foundation Topics 177

VPN Fundamentals 177

IPsec VPNs 179

SSL VPNs 181

GRE Tunnels 181

GRE Tunnel Concepts 182

Routing over GRE Tunnels 182

GRE Tunnels over the Unsecured Network 183

Configuring GRE Tunnels 185

Verifying a GRE Tunnel 187

Review Activities 190

#### Part II Review 194

#### Part III: IP Version 4 Routing Protocols 199

#### Chapter 8 Implementing OSPF for IPv4 200

Foundation Topics 201

OSPF Protocols and Operation 201

OSPF Overview 201

Becoming Neighbors and Exchanging the LSDB 202

Agreeing to Become Neighbors 202

Fully Exchanging LSAs with Neighbors 203

Maintaining Neighbors and the LSDB 204

Using Designated Routers on Ethernet Links 205

Scaling OSPF Using Areas 206

OSPF Areas 207

How Areas Reduce SPF Calculation Time 208

OSPF Area Design Advantages 209

Link-State Advertisements 209

Router LSAs Build Most of the Intra-Area Topology 210

Network LSAs Complete the Intra-Area Topology 211

LSAs in a Multi-Area Design 212

Calculating the Best Routes with SPF 214

Administrative Distance 215

OSPF Configuration and Verification 216

OSPFv2 Configuration Overview 216

Multi-Area OSPFv2 Configuration Example 217

Single-Area Configurations 218

Multi-Area Configuration 219

Verifying the Multi-Area Configuration 220

Verifying the Correct Areas on Each Interface on an ABR 221

Verifying Which Router Is DR and BDR 221

Verifying the Number and Type of LSAs 222

Verifying OSPF Routes 223

OSPF Metrics (Cost) 223

Setting the Cost Based on Interface Bandwidth 224

The Need for a Higher Reference Bandwidth 225

OSPF Load Balancing 225

Review Activities 226

#### **Chapter 9** Understanding EIGRP Concepts 230

Foundation Topics 231

EIGRP and Distance Vector Routing Protocols 231

Introduction to EIGRP 231

Basic Distance Vector Routing Protocol Features 233

The Concept of a Distance and a Vector 233

Full Update Messages and Split Horizon 234

Route Poisoning 236

EIGRP as an Advanced DV Protocol 237

EIGRP Sends Partial Update Messages, As Needed 237

EIGRP Maintains Neighbor Status Using Hello 237

Summary of Interior Routing Protocol Features 238

EIGRP Concepts and Operation 239

EIGRP Neighbors 239

Exchanging EIGRP Topology Information 240

Calculating the Best Routes for the Routing Table 241

The EIGRP Metric Calculation 241

An Example of Calculated EIGRP Metrics 242

Caveats with Bandwidth on Serial Links 243

EIGRP Convergence 244

Feasible Distance and Reported Distance 244

EIGRP Successors and Feasible Successors 245

The Query and Reply Process 246

Review Activities 248

#### Implementing EIGRP for IPv4 252 Chapter 10

Foundation Topics 253

Core EIGRP Configuration and Verification 253

EIGRP Configuration 253

Configuring EIGRP Using a Wildcard Mask 255

Verifying EIGRP Core Features 255

Finding the Interfaces on Which EIGRP Is Enabled 256

Displaying EIGRP Neighbor Status 258

Displaying the IPv4 Routing Table 259

EIGRP Metrics, Successors, and Feasible Successors 260 Viewing the EIGRP Topology Table 261 Finding Successor Routes 262 Finding Feasible Successor Routes 263 Convergence Using the Feasible Successor Route 265 Examining the Metric Components 266 Other EIGRP Configuration Settings 267 Load Balancing Across Multiple EIGRP Routes 267 Tuning the EIGRP Metric Calculation 269 Autosummarization and Discontiguous Classful Networks 270 Automatic Summarization at the Boundary of a Classful Network 270 Discontiguous Classful Networks 271 Review Activities 273 Chapter 11 Troubleshooting IPv4 Routing Protocols 278 Foundation Topics 279 Perspectives on Troubleshooting Routing Protocol Problems 279 Interfaces Enabled with a Routing Protocol 280 EIGRP Interface Troubleshooting Examining Working EIGRP Interfaces 282 Examining the Problems with EIGRP Interfaces 284 OSPF Interface Troubleshooting 286 Neighbor Relationships 289 EIGRP Neighbor Verification Checks 290 EIGRP Neighbor Troubleshooting Example 291 OSPF Neighbor Troubleshooting 293 Finding Area Mismatches 294 Finding Duplicate OSPF Router IDs 295 Finding OSPF Hello and Dead Timer Mismatches 296 Other OSPF Issues 297 Mismatched OSPF Network Types 297 Mismatched MTU Settings 299 Review Activities 300 Part III Review 304 Part IV: Wide-Area Networks 309 Chapter 12 Implementing Point-to-Point WANs 310 Foundation Topics 311 Leased Line WANs with HDLC 311 Layer 1 Leased Lines 311 The Physical Components of a Leased Line 312

Leased Lines and the T-Carrier System 314

The Role of the CSU/DSU 315

Building a WAN Link in a Lab 315

Layer 2 Leased Lines with HDLC 316

Configuring HDLC 317

Leased-Line WANs with PPP 320

PPP Concepts 320

PPP Framing 321

PPP Control Protocols 321

PPP Authentication 322

Configuring PPP 323

CHAP Configuration and Verification 324

Troubleshooting Serial Links 325

Troubleshooting Layer 1 Problems 325

Troubleshooting Layer 2 Problems 326

Keepalive Failure 327

PAP and CHAP Authentication Failure 328

Troubleshooting Layer 3 Problems 329

Review Activities 331

#### Chapter 13 Understanding Frame Relay Concepts 336

Foundation Topics 337

Frame Relay Overview 337

Virtual Circuits 339

LMI and Encapsulation Types 340

Frame Relay Encapsulation and Framing 341

Frame Relay Addressing 342

Frame Relay Local Addressing 342

Frame Forwarding with One DLCI Field 343

Network Layer Addressing with Frame Relay 344

Frame Relay Layer 3 Addressing: One Subnet Containing All Frame Relay

Frame Relay Layer 3 Addressing: One Subnet Per VC 345

Frame Relay Layer 3 Addressing: Hybrid Approach 347

Review Activities 349

#### Chapter 14 Implementing Frame Relay 352

Foundation Topics 353

Frame Relay Configuration and Verification 353

Planning a Frame Relay Configuration 353

Configuring Using Physical Interfaces and One IP Subnet 354

Configuring the Encapsulation and LMI 356

Frame Relay Address Mapping 357

Inverse ARP 360

Static Frame Relay Mapping 360

Configuring Point-to-Point Subinterfaces 361

Verifying Point-to-Point Frame Relay 364

Configuring with Multipoint Subinterfaces 366

OSPF Issues on Frame Relay Multipoint and Physical Interfaces 368

Frame Relay Troubleshooting 369

A Suggested Frame Relay Troubleshooting Process 369

Layer 1 Issues on the Access Link (Step 1) 370

Layer 2 Issues on the Access Link (Step 2) 371

PVC Problems and Status (Step 3) 372

Find the Connected Subnet and Outgoing Interface (Steps 3a and 3b) 373

Find the PVCs Assigned to That Interface (Step 3c) 374

Determine Which PVC Is Used to Reach a Particular Neighbor (Step 3d) 375

PVC Status 375

Subinterface Status 377

Frame Relay Mapping Issues (Step 4) 377

End-to-End Encapsulation (Step 5) 378

Mismatched Subnet Numbers (Step 6) 379

Review Activities 380

#### Chapter 15 Identifying Other Types of WANs 386

Foundation Topics 387

Private WANs to Connect Enterprises 387

Leased Lines 387

Frame Relay 388

Ethernet WANs 389

MPLS 390

VSAT 391

Public WANs and Internet Access 392

Internet Access (WAN) Links 392

Dial Access with Modems and ISDN 393

Digital Subscriber Line 395

Cable Internet 396

Mobile Phone Access with 3G/4G 397

PPP over Ethernet 398

PPP over Ethernet Concepts 398

PPP over Ethernet Configuration 399

Review Activities 401

#### Part IV Review 404

#### Part V: IP Version 6 409

#### Chapter 16 Troubleshooting IPv6 Routing 410

Foundation Topics 411

Normal IPv6 Operation 411

Unicast IPv6 Addresses and IPv6 Subnetting 411

Assigning Addresses to Hosts 413

Stateful DHCPv6 413

Stateless Address Autoconfiguration 414

Router Address and Static Route Configuration 415

Configuring IPv6 Routing and Addresses on Routers 415

IPv6 Static Routes on Routers 416

Verifying IPv6 Connectivity 417

Verifying Connectivity from IPv6 Hosts 417

Verifying IPv6 from Routers 419

Troubleshooting IPv6 421

Pings from the Host Work Only in Some Cases 421

Pings Fail from a Host to Its Default Router 423

Problems Using Any Function That Requires DNS 424

Host Is Missing IPv6 Settings: Stateful DHCP Issues 424

Host Is Missing IPv6 Settings: SLAAC Issues 425

Traceroute Shows Some Hops, But Fails 427

Routing Looks Good, But Traceroute Still Fails 428

Review Activities 430

#### Chapter 17 Implementing OSPF for IPv6 434

Foundation Topics 435

OSPFv3 Configuration 435

OSPFv3 ICND1 Configuration Review 435

Example Multi-Area OSPFv3 Configuration 435

Single Area Configuration on the Three Internal Routers 436

Adding Multi-Area Configuration on the Area Border Router 438

Other OSPFv3 Configuration Settings 439

Setting OSPFv3 Interface Cost to Influence Route Selection 439

OSPF Load Balancing 440

Injecting Default Routes 440

OSPF Concepts, Verification, and Troubleshooting 441

OSPFv3 Interfaces 443

Verifying OSPFv3 Interfaces 443

Troubleshooting OSPFv3 Interfaces 443

OSPFv3 Neighbors 445

Verifying OSPFv3 Neighbors 445

Troubleshooting OSPFv3 Neighbors 446

OSPFv3 LSDB and LSAs 448

Verifying OSPFv3 LSAs 448

Troubleshooting OSPFv3 LSAs 450

OSPFv3 Metrics and IPv6 Routes 451

Verifying OSPFv3 Interface Cost and Metrics 451

Troubleshooting IPv6 Routes Added by OSPFv3 453

Review Activities 455

#### Chapter 18 Implementing EIGRP for IPv6 460

Foundation Topics 461 EIGRPv6 Configuration 4

EIGRPv6 Configuration Basics 461

EIGRPv6 Configuration Example 462

Other EIGRPv6 Configuration Settings 464

Setting Bandwidth and Delay to Influence EIGRPv6 Route Selection 464

EIGRP Load Balancing 465

EIGRP Timers 466

EIGRPv6 Concepts, Verification, and Troubleshooting 466

EIGRPv6 Interfaces 467

EIGRPv6 Neighbors 469

EIGRPv6 Topology Database 470

EIGRPv6 IPv6 Routes 472

Review Activities 474

#### Part V Review 480

#### Part VI: Network Management 485

#### Chapter 19 Managing Network Devices 486

Foundation Topics 487

Simple Network Management Protocol 487

Describing SNMP 487

The Management Information Base 488

Configuring SNMP Version 2c 490

SNMP Version 3 491

System Message Logging (Syslog) 492

An Overview of System Message Logging 492

System Message Format 493

System Message Severity Levels 494

Configuring and Verifying Syslog 494

Using a Syslog Server 495

NetFlow 495

An Overview of NetFlow 496

Network Flows 497

Configuring NetFlow 497

Verifying and Using NetFlow 498 The NetFlow Collector 500

Review Activities 501

#### Chapter 20 Managing IOS Files 504

Foundation Topics 505

Managing Cisco IOS Files 505

Upgrading a Cisco IOS Software Image into Flash Memory 505

The Cisco IOS Software Boot Sequence 507

The Three Router Operating Systems 508

The Configuration Register 509

How a Router Chooses Which OS to Load 509

Recovering If the IOS Does Not Load 511

Verifying the IOS Image Using the show version Command 512

Password Recovery 513

The General Ideas Behind Cisco Password Recovery/Reset 514

A Specific Password Reset Example 515

Managing Configuration Files 517

Configuration File Basics 517

Copying and Erasing Configuration Files 519

Initial Configuration (Setup Mode) 521

Review Activities 522

#### Chapter 21 Managing IOS Licensing 526

Foundation Topics 527

IOS Packaging 527

IOS Images per Model, Series, and per Software Version/Release 527

Original Packaging: One IOS Image per Feature Set Combination 528

New IOS Packaging: One Universal Image with All Feature Sets 528

IOS Software Activation with Universal Images 529

Managing Software Activation with Cisco License Manager 530

Manually Activating Software Using Licenses 531

Example of Manually Activating a License 533

Showing the Current License Status 533

Adding a Permanent Technology Package License 535

Right-to-Use Licenses 536

Review Activities 539

#### Part VI Review 542

#### Part VII: Final Review 545

#### Chapter 22 Final Review 546

Advice About the Exam Event 546

Learn the Question Types Using the Cisco Certification Exam Tutorial 546

Think About Your Time Budget Versus Numbers of Questions 547

A Suggested Time-Check Method 548

Miscellaneous Pre-Exam Suggestions 548

Exam-Day Advice 548

Exam Review 549

Practice Subnetting and Other Math-Related Skills 549

Take Practice Exams 551

Practicing Taking the ICND2 Exam 551

Practicing Taking the CCNA Exam 552

Advice on How to Answer Exam Questions 553

Find Knowledge Gaps Through Question Review 554

Practice Hands-On CLI Skills 556

Review Mind Maps from Part Review 557

Do Labs 557

Other Study Tasks 558

Final Thoughts 558

#### Part VIII: Appendixes 561

Appendix A Numeric Reference Tables 563

Appendix B ICND2 Exam Updates 571

Glossary 598

Index 618

#### **DVD-Only Appendixes**

**Appendix C** Answers to the Review Questions

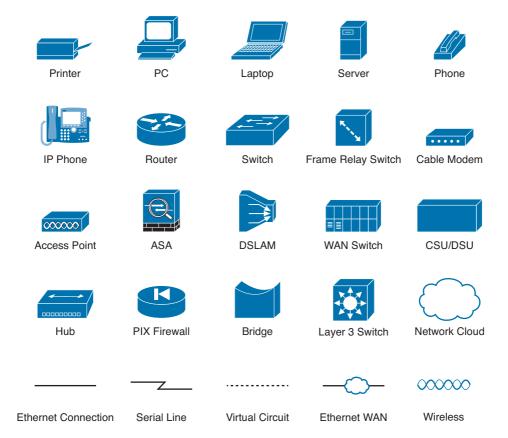
Appendix D Memory Tables

Appendix E Memory Tables Answer Key

Appendix F Mind Map Solutions

Appendix G Study Planner

#### **Icons Used in This Book**



#### **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).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars () separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

### Introduction

#### **About the Book and the Exams**

This book serves first as a textbook in some college networking courses. At the same time, you might want a career in networking somewhere down the road, and this book helps you with a big step in that journey by helping you pass a Cisco certification exam.

If you want to succeed as a technical person in the networking industry at all, you need to know Cisco. Cisco has a ridiculously high market share in the router and switch marketplace, with more than 80 percent market share in some markets. In many geographies and markets around the world, networking equals Cisco. If you want to be taken seriously as a network engineer, Cisco certification makes perfect sense.

#### The Exams That Help You Achieve CCENT and CCNA

Cisco announced changes to the CCENT and CCNA Routing and Switching certifications, and the related 100-101 ICND1, 200-101 ICND2, and 200-120 CCNA exams, early in the year 2013. For those of you who understand how the old Cisco ICND1, ICND2, and CCNA exams worked, the structure remains the same. For those of you new to Cisco certifications, this introduction begins by introducing the basics.

Most everyone new to Cisco certifications begins with either CCENT or CCNA Routing and Switching. CCENT certification requires knowledge and skills on about half as much material as does CCNA Routing and Switching, so CCENT is the easier first step.

The CCENT certification requires a single step: pass the ICND1 exam. Simple enough.

The CCNA Routing and Switching certification gives you two options, as shown in Figure I-1: pass both the ICND1 and ICND2 exams, or just pass the CCNA exam. (Note that there is no separate certification for passing the ICND2 exam.)

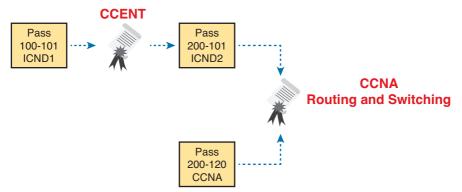


Figure I-1 Cisco Entry-Level Certifications and Exams

As you can see, although you can obtain the CCENT certification by taking the ICND1 exam, you do not have to be CCENT certified before you get your CCNA Routing and Switching certification. You can choose to take the CCNA exam and bypass the CCENT certification.

As for the topics themselves, the ICND1 and ICND2 exams cover different topics (but with some overlap required). For example, ICND1 covers the basics of the Open Shortest Path First (OSPF) routing protocol. ICND2 covers more detail about OSPF, but to discuss those additional details,

ICND2 must rely on the parts of OSPF included in ICND1. Many topics in ICND2 build on topics in ICND1, causing some overlap.

The CCNA exam covers all the topics in both ICND1 and ICND2, no more, no less.

#### Types of Questions on the Exams

The ICND1, ICND2, and CCNA exams all follow the same general format. At the testing center, you sit in a quiet room with a PC. Before the exam timer begins, you have a chance to do a few other tasks on the PC; for instance, you can take a sample quiz just to get accustomed to the PC and the testing engine. Anyone who has user-level skills in getting around a PC should have no problems with the testing environment.

Once the exam starts, the screen shows you question after question. The questions usually fall into one of the following categories:

- Multiple choice, single answer
- Multiple choice, multiple answer
- Testlet
- Drag-and-drop
- Simulated lab (sim)
- Simlet

The first three items in the list are all multiple choice questions. The multiple choice format simply requires that you point and click a circle beside the correct answer(s). Cisco traditionally tells you how many answers you need to choose, and the testing software prevents you from choosing too many answers. The testlet style gives you one larger scenario statement, with multiple different multiple choice questions about that one scenario.

Drag-and-drop questions require you to move some items around on the GUI. You left-click and hold, move a button or icon to another area, and release the clicker to place the object somewhere else—usually into a list. So, for some questions, to answer the question correctly, you might need to put a list of five things in the proper order.

The last two types both use a network simulator to ask questions. Interestingly, the two types actually allow Cisco to assess two very different skills. First, sim questions generally describe a problem, and your task is to configure one or more routers and switches to fix the problem. The exam then grades the question based on the configuration you changed or added.

The simlet questions may well be the most difficult style of question on the exams. Simlet questions also use a network simulator, but instead of you answering the question by changing the configuration, the question includes one or more multiple choice questions. The questions require that you use the simulator to examine the current behavior of a network, interpreting the output of any show commands that you can remember to answer the question. Whereas sim questions require you to troubleshoot problems related to a configuration, simlets require you to analyze both working and broken networks, correlating show command output with your knowledge of networking theory and configuration commands.

You can watch and even experiment with these command types using the Cisco Exam Tutorial. To find the Cisco Certification Exam Tutorial, go to http://www.cisco.com and search for "exam tutorial."

#### What's on the CCNA Exams?

Ever since I was in grade school, whenever the teacher announced that we were having a test soon, someone would always ask, "What's on the test?" Even in college, people would try to get more information about what would be on the exams. At heart, the goal is to know what to study hard, what to study a little, and what to not study at all.

Cisco tells the world the topics on each of their exams. Cisco wants the public to know both the variety of topics, and an idea about the kinds of knowledge and skills required for each topic, for every Cisco certification exam. To that end, Cisco publishes a set of exam topics for each exam.

Many Cisco exam topics list both a networking topic plus an important verb. The verb tells us to what degree the topic must be understood and what skills are required. The topic also implies the kinds of skills required for that topic. For example, one topic might start with "Describe...," another with "Configure...," another with "Verify...," and another might begin with Troubleshoot...." That last topic has the highest required skill level, because to troubleshoot you must understand the topic, be able to configure it (to see what's wrong with the configuration), and verify it (to find the root cause of the problem). By listing the topics and skill level, Cisco helps us all prepare for its exams. Although the exam topics are helpful, keep in mind that Cisco adds a disclaimer that the posted exam topics for all of its certification exams are guidelines. Cisco makes the effort to keep the exam questions within the confines of the stated exam topics, and I know from talking to those involved that every question is analyzed for whether it fits within the stated exam topics.

#### **ICND1 Exam Topics**

Tables I-1 through I-7 list the exam topics for the ICND1 exam. Following those tables, Tables I-8 through I-12 list the exam topics for ICND2. These tables note the book chapters in which each exam topic is covered.

Note that the tables follow Cisco's organization of topics, by both grouping similar topics and listing sub-topics. The subtopics simply give more specific terms and concepts to provide more detail about some exam topics. The tables show the main topics in bold and the subtopics as indented text inside the tables.

Table I-1	ICND1 Fxam	Topics: Operation	of IP Data	Networks

Chapter	Operation of IP Data Networks
1–4, 6, 15	Recognize the purpose and functions of various network devices such as Routers, Switches, Bridges and Hubs.
1-4, 6, 15	Select the components required to meet a given network specification.
5	Identify common applications and their impact on the network
1	Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models.
2-5, 6, 9, 16, 24, 25	Predict the data flow between two hosts across a network.
2, 6, 15	Identify the appropriate media, cables, ports, and connectors to connect Cisco network devices to other network devices and hosts in a LAN

Table I-2 ICND1 Exam Topics: LAN Switching Technologies

Chapter	LAN Switching Technologies
2, 6	Determine the technology and media access control method for Ethernet networks
6, 8, 9	Identify basic switching concepts and the operation of Cisco switches.
6, 8	Collision Domains

Chapter	LAN Switching Technologies
6, 9	Broadcast Domains
6	Types of switching
6, 8, 9	CAM Table
7	Configure and verify initial switch configuration including remote access management.
7	Cisco IOS commands to perform basic switch setup
7, 18, 28	Verify network status and switch operation using basic utilities such as ping, telnet and ssh.
9	Describe how VLANs create logically separate networks and the need for routing between them.
9	Explain network segmentation and basic traffic management concepts
9	Configure and verify VLANs
9, 10	Configure and verify trunking on Cisco switches
9, 10	DTP
10	Auto negotiation

Table I-3 ICND1 Exam Topics: IP Addressing (IPv4/IPv6)

Chapter	IP Addressing (IPv4/IPv6)
11	Describe the operation and necessity of using private and public IP addresses for IPv4 addressing
25, 26	Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment.
11, 19, 20, 21	Identify the appropriate IPv4 addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment.
27, 28, 29	Describe the technological requirements for running IPv6 in conjunction with IPv4 such as dual stack
25–28	Describe IPv6 addresses
25, 26	Global unicast
27	Multicast
27	Link local
26	Unique local
27	eui 64
28	autoconfiguration

Table I-4 ICND1 Exam Topics: IP Routing Technologies

Chapter	IP Routing Technologies
16	Describe basic routing concepts
16	CEF
16	Packet forwarding
16	Router lookup process
15–18, 27	Configure and verify utilizing the CLI to set basic Router configuration
16–18, 27	Cisco IOS commands to perform basic router setup
16, 27	Configure and verify operation status of an ethernet interface
16–18, 27–29	Verify router configuration and network connectivity
16–18, 27, 29	Cisco IOS commands to review basic router information and network connectivity
16, 29	Configure and verify routing configuration for a static or default route given specific routing requirements
4, 16, 17, 25, 29	Differentiate methods of routing and routing protocols
4, 17, 29	Static vs. Dynamic
17	Link state vs. Distance Vector
16, 25	next hop
16, 25	ip routing table
17, 29	Passive interfaces
17, 29	Configure and verify OSPF (single area)
17, 29	Benefit of single area
17	Configure OSPF v2
29	Configure OSPF v3
17, 29	Router ID
17, 29	Passive interface
16	Configure and verify interVLAN routing (Router on a stick)
16	sub interfaces
16	upstream routing
16	encapsulation
8, 16	Configure SVI interfaces

Table I-5 ICND1 Exam Topics: IP Services

Chapter	IP Services
18, 28	Configure and verify DHCP (IOS Router)
18, 28	configuring router interfaces to use DHCP
18	DHCP options
18	excluded addresses

Chapter	IP Services
18	lease time
22, 23	Describe the types, features, and applications of ACLs
22	Standard
23	Sequence numbers
23	Editing
23	Extended
23	Named
22, 23	Numbered
22	Log option
22, 23	Configure and verify ACLs in a network environment
23	Named
22, 23	Numbered
22	Log option
24	Identify the basic operation of NAT
24	Purpose
24	Pool
24	Static
24	1 to 1
24	Overloading
24	Source addressing
24	One way NAT
24	Configure and verify NAT for given network requirements
23	Configure and verify NTP as a client

Table I-6 ICND1 Exam Topics: Network Device Security

Chapter	Network Device Security
8, 15	Configure and verify network device security features such as
8, 15	Device password security
8, 15	Enable secret vs enable
23	Transport
23	Disable telnet
8	SSH
8	VTYs
23	Physical security
8	Service password
8	Describe external authentication methods

Chapter	Network Device Security
8, 10	Configure and verify Switch Port Security features such as
8	Sticky MAC
8	MAC address limitation
8, 10	Static / dynamic
8, 10	Violation modes
8, 10	Err disable
8, 10	Shutdown
8, 10	Protect restrict
8	Shutdown unused ports
8	Err disable recovery
8	Assign unused ports to an unused VLAN
23	Setting native VLAN to other than VLAN 1
22, 23	Configure and verify ACLs to filter network traffic
23	Configure and verify an ACLs to limit telnet and SSH access to the router

Table I-7 ICND1 Exam Topics: Troubleshooting

Chapter	Troubleshooting
12–15, 18–21, 25–28	Troubleshoot and correct common problems associated with IP addressing and host configurations.
9, 10	Troubleshoot and Resolve VLAN problems
9, 10	identify that VLANs are configured
9, 10	port membership correct
9, 10	IP address configured
9, 10	Troubleshoot and Resolve trunking problems on Cisco switches
9, 10	correct trunk states
9, 10	correct encapsulation configured
9, 10	correct vlans allowed
22, 23	Troubleshoot and Resolve ACL issues
22, 23	Statistics
22, 23	Permitted networks
22, 23	Direction
22, 23	Interface
10	Troubleshoot and Resolve Layer 1 problems
10	Framing
10	CRC
10	Runts

Chapter	Troubleshooting
10	Giants
10	Dropped packets
10	Late collision
10	Input / Output errors

#### **ICND2** Exam Topics

Tables I-8 through I-12 list the exam topics for ICND2. These tables note the book chapters in which each exam topic is covered. Note that each table covers a main exam topic. Cisco released further information about each topic to several sublevels of hierarchy. In this table, those sublevels are indented to indicate the topic above them they are related to.

Table I-8 ICND2 Exam Topics: LAN Switching Technologies

Chapters	LAN Switching Technologies
1	Identify enhanced switching technologies
1	RSTP
1	PVSTP
1	Etherchannels
1, 2	Configure and verify PVSTP operation
1, 2	describe root bridge election
2	spanning tree mode

Table I-9 ICND2 Exam Topics, IP Routing Technologies

Chapters	IP Routing Technologies
20	Describe the boot process of Cisco IOS routers
20	POST
20	Router bootup process
12	Configure and verify operation status of a Serial interface.
20, 21	Manage Cisco IOS Files
20	Boot preferences
20	Cisco IOS image(s)
21	Licensing
21	Show license
21	Change license
8-11, 16-18	Differentiate methods of routing and routing protocols
8	Administrative distance
9	split horizon
8, 9, 17, 18	metric
8, 9, 17, 18	next hop

Chapters	IP Routing Technologies
8, 17	Configure and verify OSPF (single area)
8, 11, 17	neighbor adjacencies
8, 11, 17	OSPF states
8, 17	Discuss Multi area
8	Configure OSPF v2
17	Configure OSPF v3
8, 17	Router ID
8, 17	LSA types
9, 10, 18	Configure and verify EIGRP (single AS)
9, 10, 18	Feasible Distance / Feasible Successors /Administrative distance
9, 18	Feasibility condition
9, 18	Metric composition
9, 10, 18	Router ID
9, 10	Auto summary
9, 10, 18	Path selection
9, 10, 18	Load balancing
9, 10, 18	Equal
9, 10, 18	Unequal
9, 10, 18	Passive interface

Table I-10 ICND2 Exam Topics, IP Services

Chapters	IP Services
6	Recognize High availability (FHRP)
6	VRRP
6	HSRP
6	GLBP
19	Configure and verify Syslog
19	Utilize Syslog Output
19	Describe SNMP v2 & v3

Table I-11 ICND2 Exam Topics, Troubleshooting

Chapters	Troubleshooting
3–5, 16	Identify and correct common network problems
19	Utilize netflow data
2	Troubleshoot and Resolve Spanning Tree operation issues
2	root switch
2	priority

Chapters	Troubleshooting		
2	mode is correct		
2	port states		
4, 5, 16	Troubleshoot and Resolve routing issues		
4, 5, 16	routing is enabled		
4, 5, 16	routing table is correct		
4, 5, 16	correct path selection		
11, 17	Troubleshoot and Resolve OSPF problems		
11, 17	neighbor adjacencies		
11, 17	Hello and Dead timers		
11, 17	OSPF area		
11, 17	Interface MTU		
11, 17	Network types		
11, 17	Neighbor states		
11, 17	OSPF topology database		
11, 18	Troubleshoot and Resolve EIGRP problems		
11, 18	neighbor adjacencies		
11, 18	AS number		
11, 18	Load balancing		
11, 18	Split horizon		
3, 5	Troubleshoot and Resolve interVLAN routing problems		
5	Connectivity		
5	Encapsulation		
5	Subnet		
3, 5	Native VLAN		
3, 5	Port mode trunk status		
12, 14	Troubleshoot and Resolve WAN implementation issues		
12	Serial interfaces		
12	PPP		
14	Frame relay		
19	Monitor NetFlow statistics		
2	Troubleshoot etherchannel problems		

Chapters	WAN Technologies	
7, 13, 15	Identify different WAN Technologies	
15	Metro Ethernet	
15	VSAT	
15	Cellular 3G / 4G	
15	MPLS	
12, 15	T1 / E1	
15	ISDN	
15	DSL	
13	Frame relay	
15	Cable	
7	VPN	
12	Configure and verify a basic WAN serial connection	
12	Configure and verify a PPP connection between Cisco routers	
14	Configure and verify Frame Relay on Cisco routers	

Table I-12 ICND2 Exam Topics: WAN Technologies

#### CCNA Exam Topics

15

The 200-120 CCNA exam actually covers everything from both the ICND1 and ICND2 exams, at least based on the published exam topics. As of publication, the CCNA exam topics include all topics in Tables I-1 through I-12. In short, CCNA = ICND1 + ICND2.

Implement and troubleshoot PPPoE

**NOTE** Because it is possible that the exam topics may change over time, it might be worth the time to double-check the exam topics as listed on the Cisco website (http://www.cisco.com/go/ ccent and http://www.cisco.com/go/ccna). If Cisco does happen to add exam topics at a later date, note that Appendix B, "ICND2 Exam Updates," describes how to go to http://www.ciscopress.com and download additional information about those newly added topics.

# **About the Book**

This book discusses the content and skills needed to pass the 200-101 ICND2 exam. That content also serves as basically the second half of the CCNA content, with this book's companion title, the Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition, discussing the first half of the content.

Each of these books uses the same kinds of book features, so if you are reading both this book and the ICND1 book, you do not need to read the Introduction to the other book. Also, for those of you using both books to prepare for the 200-120 CCNA exam (rather than taking the two-exam option), the end of this Introduction lists a suggested reading plan.

#### **Book Features**

The most important and somewhat obvious objective of this book is to help you pass the ICND2 exam or the CCNA exam. In fact, if the primary objective of this book were different, the book's title would be misleading! However, the methods used in this book to help you pass the exams are also designed to make you much more knowledgeable about how to do your job.

This book uses several tools to help you discover your weak topic areas, to help you improve your knowledge and skills with those topics, and to prove that you have retained your knowledge of those topics. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. The CCNA certification is the foundation for many of the Cisco professional certifications, and it would be a disservice to you if this book did not help you truly learn the material. Therefore, this book helps you pass the CCNA exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the DVD

#### **Chapter Features**

To help you customize your study time using these books, the core chapters have several features that help you make the best use of your time:

- Introduction and Exam Topics: Each chapter begins with an introduction to the chapter's main topics and a listing of the official exam topics that are covered in that chapter.
- Foundation Topics: These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- Review Activities: At the end of the "Foundation Topics" section of each chapter, the "Review Activities" section lists a series of study activities that should be done at the end of the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include the following:
  - Chapter Summaries: This is a thorough summary of the main chapter topics for you to review. Make sure you understand all these points in detail, and refer to the chapter if not.
  - Review Questions: These questions offer a chance for you to assess how well you retained particular facts from the Foundation Topics.
  - Review Key Topics: The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Key Topics Review activity lists the key topics from the chapter and their corresponding page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic.
  - Complete Tables and Lists from Memory: To help you exercise your memory and memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the DVD. This document lists only partial information, allowing you to complete the table or list.
  - Define Key Terms: Although the exams may be unlikely to ask a question like "Define this term," the CCNA exams require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary at the end of this book.

■ Command Reference Tables: Some book chapters cover a large amount of configuration and EXEC commands. These tables list the commands introduced in the chapter, along with an explanation. For exam preparation, use it for reference, but also read the table once when performing the Review Activities to make sure that you remember what all the commands do.

#### Part Review

The Part Review tasks help you prepare to apply all the concepts in each respective part of the book. (Each book part contains a number of related chapters.) The Part Review includes sample test questions, which require you to apply the concepts from multiple chapters in that part, uncovering what you truly understood and what you did not quite yet understand. The Part Review also uses mind map exercises that help you mentally connect concepts, configuration, and verification, so that no matter what perspective a single exam question takes, you can analyze and answer the question.

The Part Reviews list tasks, along with checklists, so you can track your progress. The following list explains the most common tasks you will see in the Part Review; note that not all Part Reviews use every type of task.

- Repeat Chapter Review: Although you have already seen the chapter review questions from the chapters in a part, re-answering those questions can prove a useful way to review facts. The Part Review suggests that you repeat the chapter review questions, but using the Pearson IT Certification Practice Test (PCPT) exam software that comes with the book, for extra practice in answering multiple choice questions on a computer.
- Answer Part Review Questions: The PCPT exam software includes several exam databases. One exam database holds Part Review questions, written specifically for Part Review. These questions purposefully include multiple concepts in each question, sometimes from multiple chapters, to help build the skills needed for the more challenging analysis questions on the exams.
- Review Key Topics: Yes, again! They are indeed the most important topics in each chapter.
- Create Configuration Mind Maps: Mind maps are graphical organizing tools that many people find useful when learning and processing how concepts fit together. The process of creating mind maps helps you build mental connections between concepts and configuration commands, as well as develop your recall of the individual commands. For this task, you may create the mind map on paper or using any mind mapping or graphic organizer software. (For more information about mind maps, see the section "About Mind Maps and Graphic Visualization" in the Introduction of this book.)
- Create Verification Mind Maps: These mind mapping exercises focus on helping you connect router and switch show commands to either networking concepts or to configuration commands. Simply create the mind maps on paper or using any mind mapping or graphic organizer software.
- Repeat Chapter Review Tasks (Optional): Browse through all the Review Activities, and repeat any that you think might help you with review at this point.

#### Final Prep Tasks

Chapter 22, at the end of this book, lists a series of preparation tasks that you can best use for your final preparation before taking the exam.

#### Other Features

In addition to the features in each of the core chapters, this book, as a whole, has additional study resources, including the following:

■ DVD-based practice exam: The companion DVD contains the powerful Pearson IT Certification Practice Test exam engine. You can take simulated ICND2 exams, as well as

- simulated CCNA exams, with the DVD and activation code included in this book. (You can take simulated ICND1 and CCNA exams with the DVD in the Cisco CCENT/CCNA ICND1 Official Cert Guide, Academic Edition.)
- CCNA ICND2 Simulator Lite: This lite version of the best-selling CCNA Network Simulator from Pearson provides you with a means, right now, to experience the Cisco command-line interface (CLI). No need to go buy real gear or buy a full simulator to start learning the CLI. Just install it from the DVD in the back of this book.
- eBook: This Academic Edition comes complete with a free copy of the Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide Premium Edition eBook and Practice Test. The Premium Edition eBook provides you with three different eBook files: PDF, EPUB, and Mobi (native Kindle format). In addition, the Premium Edition enables you to link all the questions from the practice test software to the PDF file of the book, so you can link directly to the book content from each question for further study. Instructions for accessing your Premium Edition can be found on the access code card in the DVD sleeve.
- Mentoring videos: The DVD included with this book includes four other instructional videos, about the following topics: OSPF, EIGRP, EIGRP Metrics, plus PPP and CHAP.
- Companion website: The website http://www.ciscopress.com/title/1587143739 posts up-tothe-minute materials that further clarify complex exam topics. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam.
- PearsonITCertification.com: The website http://www.pearsonitcertification.com is a great resource for all things IT-certification related. Check out the great CCNA articles, videos, blogs, and other certification preparation tools from the industry's best authors and trainers.
- CCNA Simulator: If you are looking for more hands-on practice, you might want to consider purchasing the CCNA Network Simulator. You can purchase a copy of this software from Pearson at http://pearsonitcertification.com/networksimulator or other retail outlets. To help you with your studies, I have created a mapping guide that maps each of the labs in the simulator to the specific sections in these CCNA cert guides. You can get this mapping guide for free on the Extras tab of the companion website.
- Author's website and blogs: The author maintains a website that hosts tools and links useful when studying for CCENT and CCNA. The site lists information to help you build your own lab, study pages that correspond to each chapter of this book and the ICND1 book, and links to the author's CCENT Skills blog and CCNA Skills blog. Start at http://www.certskills.com; check the tabs for study and blogs in particular.

# **Book Organization, Chapters, and Appendices**

This book contains 21 core chapters, Chapters 1 through 21, with Chapter 22 including some suggestions for how to approach the actual exams. Each core chapter covers a subset of the topics on the ICND2 exam. The core chapters are organized into sections. The core chapters cover the following topics:

#### Part I: LAN Switching

- Chapter 1, "Spanning Tree Protocol Concepts," discusses the concepts behind IEEE Spanning Tree Protocol (STP) and how it makes some switch interfaces block frames to prevent frames from looping continuously around a redundant switched LAN.
- Chapter 2, "Spanning Tree Protocol Implementation," shows how to configure, verify, and troubleshoot STP implementation on Cisco switches.
- Chapter 3, "Troubleshooting LAN Switching," reviews LAN switching topics from the ICND1 book, while moving toward a deeper understanding of those topics. In particular, this chapter examines the most common LAN switching issues and how to discover those issues when troubleshooting a network.

#### Part II: IP Version 4 Routing

- Chapter 4, "Troubleshooting IPv4 Routing Part I," reviews IPv4 routing, and then focuses on how to use two key troubleshooting tools to find routing problems: the ping and traceroute commands.
- Chapter 5, "Troubleshooting IPv4 Routing Part II," looks at the most common IPv4 problems and how to find the root causes of those problems when troubleshooting.
- Chapter 6, "Creating Redundant First-Hop Routers," discusses the need for a First Hop Redundancy Protocol (FHRP), how the protocols make multiple routers act like a single default router, and the configuration and verification details of both Hot Standby Router Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP).
- Chapter 7, "Virtual Private Networks," discusses the need for VPN technology when sending private network data over public networks like the Internet. It also discusses basic tunneling configuration using generic routing encapsulation (GRE) tunnels on Cisco routers.

### Part III: IP Version 4 Routing Protocols

- Chapter 8, "Implementing OSPF for IPv4," reviews the ICND1 book's coverage of OSPF Version 2 (OSPFv2). It also takes the concepts deeper, with more discussion of the OSPF processes and database and with additional configuration options.
- Chapter 9, "Understanding EIGRP Concepts," introduces the fundamental operation of the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 (EIGRPv4), focusing on EIGRP neighbor relationships, how it calculates metrics, and how it quickly converges to alternate feasible successor routes.
- Chapter 10, "Implementing EIGRP for IPv4," takes the concepts discussed in the previous chapter and shows how to configure and verify those same features.
- Chapter 11, "Troubleshooting IPv4 Routing Protocols," walks through the most common problems with IPv4 routing protocols, while alternating between OSPF examples and EIGRP examples.

#### Part IV: Wide-Area Networks

- Chapter 12, "Implementing Point-to-Point WANs," explains the core concepts of how to build a leased-line WAN and the basics of the two common data link protocols on these links: HDLC and PPP.
- Chapter 13, "Understanding Frame Relay Concepts," explains how to build a Frame Relay WAN between routers, focusing on the protocols and concepts rather than the configuration.
- Chapter 14, "Implementing Frame Relay," takes the concepts discussed in Chapter 13 and shows how to configure, verify, and troubleshoot those same features.
- Chapter 15, "Identifying Other Types of WANs," gives a broad description of many other types of WAN technology, including Ethernet WANs, Multiprotocol Label Switching (MPLS), and digital subscriber line (DSL).

#### Part V: IP Version 6

- Chapter 16, "Troubleshooting IPv6 Routing," reviews IPv6 routing as discussed in the ICND1 book. It then shows some of the most common problems with IPv6 routing and discusses how to troubleshoot these problems to discover the root cause.
- Chapter 17, "Implementing OSPF for IPv6," reviews the ICND1 book's coverage of OSPF Version 3 (OSPFv3). It then compares some deeper OSPFv3 concepts and configuration with these same concepts for OSPFv2, as discussed earlier in Chapter 8.

■ Chapter 18, "Implementing EIGRP for IPv6," takes the EIGRP concepts discussed for IPv4 in Chapter 9 and shows how those same concepts apply to EIGRP for IPv6 (EIGRPv6). It then shows how to configure and verify EIGRPv6 as well.

#### Part VI: Network Management

- Chapter 19, "Managing Network Devices," discusses the concepts and configuration of three common network management tools: Simple Network Management Protocol (SNMP), syslog, and NetFlow.
- Chapter 20, "Managing IOS Files," explains some necessary details about router internals and IOS. In particular, it discusses the boot process on a router, how a router choosing which IOS image to use, and the different locations where a router can store its IOS images.
- Chapter 21, "Managing IOS Licensing," discusses Cisco's current methods of granting a particular router the right to use a particular IOS image and feature set through the use of IOS licenses.

#### Part VII: Final Review

■ Chapter 22, "Final Review," suggests a plan for final preparation once you have finished the core parts of the book, in particular explaining the many study options available in the book.

#### Part VIII: Appendixes (In Print)

- Appendix A, "Numeric Reference Tables," lists several tables of numeric information, including a binary-to-decimal conversion table and a list of powers of 2.
- Appendix B, "ICND2 Exam Updates," covers a variety of short topics that either clarify or expand on topics covered earlier in the book. This appendix is updated from time to time and posted at http://www.ciscopress.com/title/1587143739, with the most recent version available at the time of printing included here as Appendix B. (The first page of the appendix includes instructions on how to check to see if a later version of Appendix B is available online.)
- The Glossary contains definitions for all of the terms listed in the "Definitions of Key Terms" section at the conclusion of Chapters 1 through 21.

#### Appendixes (on the DVD)

The following appendixes are available in digital format on the DVD that accompanies this book:

- Appendix C, "Answers to Review Questions," includes the explanations to all the questions from Chapters 1 through 21.
- Appendix D, "Memory Tables," holds the key tables and lists from each chapter, with some of the content removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams.
- Appendix E, "Memory Tables Answer Key," contains the answer key for the exercises in Appendix D.
- Appendix F, "Mind Map Solutions," shows an image of sample answers for all the part-ending mind map exercises.
- Appendix G, "Study Planner," is a spreadsheet with major study milestones, where you can track your progress through your study.

# **Reference Information**

This short section contains a few topics available for reference elsewhere in the book. You may read these when you first use the book, but you may also skip these topics and refer back to them later. In particular, make sure to note the final page of this introduction, which lists several contact details, including how to get in touch with Cisco Press.

# **Install the Pearson IT Certification Practice Test Engine and Questions**

The DVD in the book includes the Pearson IT Certification Practice Test (PCPT) engine—software that displays and grades a set of exam-realistic multiple choice, drag-and-drop, fill-in-the-blank, and testlet questions. Using the PCPT engine, you can either study by going through the questions in study mode or take a simulated ICND2 or CCNA exam that mimics real exam conditions.

The installation process requires two major steps. The DVD in the back of this book has a recent copy of the PCPT engine. The practice exam—the database of ICND2 and CCNA exam questions—is not on the DVD. After you install the software, the PCPT software downloads the latest versions of both the software and the question databases for this book using your Internet connection.

**NOTE** The cardboard DVD case in the back of this book includes both the DVD and a piece of thick paper. The paper lists the digital product voucher code and instructions for accessing the eBook files and the practice exams associated with this book. *Do not lose the activation code.* 

#### Redeem Your Digital Product Voucher to Access the eBook and Practice Test Code

To use the practice test software, you must first redeem your digital product voucher found on the card in the DVD sleeve. To do so, follow these steps:

- **Step 1.** If you have a Cisco Press account, go to www.ciscopress.com/account and log in. If you do not have a Cisco Press account, go to www.ciscopress.com/join and create an account.
- **Step 2.** On your Account page, find the "Digital Product Voucher" box at the top of the right column.
- **Step 3.** Type in your digital product voucher code found on the DVD card, and click Submit.

**NOTE** Codes are one-time use and may not be shared.

**Step 4.** The products and download link will now be listed under Digital Purchases on your Account page. Click the "refresh" links to generate your eBook files for download. Use the access code to unlock and download the Premium Edition practice exams in the Pearson IT Certification Practice Test software, as described in the following sections.

# Install the Software from the DVD

The software installation process is pretty routine as compared with other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from

- **Step 1.** Insert the DVD into your PC.
- **Step 2.** The software that automatically runs is the Cisco Press software to access and use all DVD-based features, including the exam engine and the DVD-only appendixes. From the main menu, click the **Install the Exam Engine** option.
- **Step 3.** Respond to windows prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the DVD sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, you do not need to register again. Just use your existing login.

#### Activate and Download the Practice Exam

When the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process), as follows:

- **Step 1.** Start the PCPT software from the Windows Start menu or from your desktop short-cut icon.
- **Step 2.** To activate and download the exam associated with this book, from the My Products or Tools tab, click the **Activate** button.
- **Step 3.** At the next screen, enter the activation key listed under the Premium Edition product on your account page on www.ciscopress.com, and then click the **Activate** button.
- **Step 4.** The activation process downloads the practice exam. Click **Next**, and then click **Finish**.

After the activation process is completed, the My Products tab should list your new exam. If you do not see the exam, make sure you have selected the My Products tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the Open Exam button.

To update a particular product's exams that you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Updating your exams ensures that you have the latest changes and updates to the exam data.

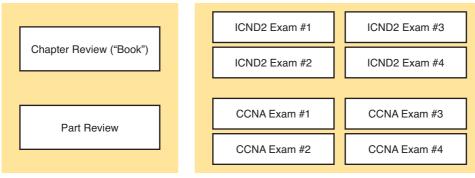
If you want to check for updates to the PCPT software, simply select the **Tools** tab and click the **Update Application** button. This will ensure that you are running the latest version of the software engine.

#### **Activating Other Products**

The exam software installation process and the registration process have to happen only once. Then for each new product, you have to complete just a few steps. For instance, if you buy another new Cisco Press Official Cert Guide or Pearson IT Certification Cert Guide, extract the activation code from the DVD sleeve in the back of that book; you don't even need the DVD at this point. From there, all you have to do is start PCPT (if not still up and running), and perform steps 2 through 4 from the previous list.

#### **PCPT Exam Databases with This Book**

The practice test questions come in different exams or exam databases. When you install the PCPT software and type in the activation code, the PCPT software downloads the latest version of all these exam databases. And with the ICND2 book alone, you get 10 different "exams," or 10 different sets of questions, as listed in Figure I-2.



Use for Part Review

Use for Exam Review

Figure I-2 PCPT Exams/Exam Databases and When to Use Them

You can choose to use any of these exam databases at any time, both in study mode and practice exam mode. However, many people find it best to save some of the exams until exam review time, after you have finished reading the entire book. Figure I-2 begins to suggest a plan, spelled out here:

- During Part Review, use PCPT to review the Chapter Review questions (designated as "Book Questions" in the software) for that part, using study mode.
- During Part Review, use the questions built specifically for Part Review (the Part Review questions) for that part of the book, using study mode.
- Save the remaining exams to use with Chapter 22, "Final Review," using practice exam mode, as discussed in that chapter.

The two modes inside PCPT give you better options for study versus practicing a timed exam event. In study mode, you can see the answers immediately, so you can study the topics more easily. Also, you can choose a subset of the questions in an exam database; for instance, you can view questions from only the chapters in one part of the book.

Practice exam mode creates an event somewhat like the actual exam. It gives you a preset number of questions, from all chapters, with a timed event. Practice exam mode also gives you a score for that timed event.

#### How to View Only Chapter Review Questions by Part

Each Part Review asks you to repeat the Chapter Review quiz questions from the chapters in that part. You can simply scan the book pages to review these questions, but it is slightly better to review these questions from inside the PCPT software, just to get a little more practice in how to read questions from the testing software. But you can just read them in the book, as well.

To view these Chapter Review (book) questions inside the PCPT software, you need to select **Book Questions**, and the chapters in this part, using the PCPT menus. To do so, follow these steps:

- **Step 1.** Start the PCPT software.
- **Step 2.** From the main (home) menu, select the item for this product, with a name like Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, and click **Open Exam.**

- Step 3. The top of the next window that appears should list some exams; check the ICND2 Book Questions box, and uncheck the other boxes. This selects the "book" questions (that is, the Chapter Review questions from the end of each chapter).
- Step 4. On this same window, click at the bottom of the screen to deselect all objectives (chapters). Then select the box beside each chapter in the part of the book you are reviewing.
- Step 5. Select any other options on the right side of the window.
- Step 6. Click **Start** to start reviewing the questions.

#### How to View Part Review Questions by Part Only

The exam databases you get with this book include a database of questions created solely for study during the Part Review process. Chapter Review questions focus more on facts, with basic application. The Part Review questions instead focus more on application and look more like real exam questions.

To view these questions, follow the same process as you did with Chapter Review/book questions, but select the Part Review database rather than the book database. Specifically, follow these steps:

- Step 1. Start the PCPT software.
- Step 2. From the main (home) menu, select the item for this product, with a name like Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, and click Open Exam.
- Step 3. The top of the next window should list some exams; check the Part Review Questions box, and uncheck the other boxes. This selects the questions intended for part-ending review.
- Step 4. On this same window, click at the bottom of the screen to deselect all objectives, and then select (check) the box beside the book part you want to review. This tells the PCPT software to give you Part Review questions from the selected part.
- Step 5. Select any other options on the right side of the window.
- Step 6. Click Start to start reviewing the questions.

# **About Mind Maps**

Mind maps are a type of visual organization tool that you can use for many purposes. For instance, you can use mind maps as an alternative way to take notes.

You can also use mind maps to improve how your brain organizes concepts. Mind maps stress the connections and relationships between ideas. When you spend time thinking about an area of study, and organize your ideas into a mind map, you strengthen existing mental connections, create new connections, all into your own frame of reference.

In short, mind maps help you internalize what you learn.

#### Mind Map Mechanics

Each mind map begins with a blank piece of paper or blank window in an application. You then add a large central idea, with branches that move out in any direction. The branches contain smaller concepts, ideas, commands, pictures, whatever idea needs to be represented. Any concepts that can be grouped should be put near each other. As need be, you can create deeper and deeper branches, although for this book's purposes, most mind maps will not go beyond a couple of levels.

**NOTE** Many books have been written about mind maps, but Tony Buzan often gets credit for formalizing and popularizing mind maps. You can learn more about mind maps at his website, http://www.thinkbuzan.com.

For example, Figure I-3 shows a sample mind map that begins to output some of the IPv6 content from Part VII of the ICND1 book. The central concept of the mind map is IPv6 addressing, and the Part Review activity asks you to think of all facts you learned about IPv6 addressing, and organize them with a mind map. The mind map allows for a more visual representation of the concepts as compared with just written notes.

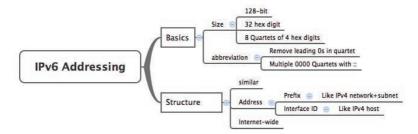


Figure I-3 Sample Mind Map

#### About Mind Maps Used During Part Review

This book suggests mind mapping exercises during Part Review. This short topic lists some details about the Part Review mind mapping exercises, listed in one place for reference.

Part Review uses two main types of mind mapping exercises:

Configuration exercises ask you to recall the related configuration commands and group them. For instance, in a configuration exercise, related commands that happen to be interface subcommands should be grouped, but as shown as being inside interface configuration mode.

Verification exercises ask you to think about the output of show commands and link the output to either the configuration commands that cause that output or the concepts that explain the meaning of some of that output.

Create these configuration mind maps on paper, using any mind mapping software, or even any drawing application. Many mind mapping apps exist as well. Regardless of how you draw them, follow these rules:

- If you have only a little time for this exercise, spend your time making your own mind map, instead of looking at suggested answers. The learning happens when thinking through the problem of making your own mind map.
- Set aside the book and all your notes, and do not look at them, when first creating these maps, and do as much as you can without looking at the book or your notes (or Google, or anything else).
- Try all the mind maps listed in a Part Review before looking at your notes.
- Finally, look at your notes to complete all the mind maps.
- Make a note of where you put your final results so that you can find them later during final exam review.

Finally, when learning to use these tools, take two other important suggestions as well. First, use as few words as possible for each node in your mind map. The point is for you to remember the idea and its connections, rather than explain the concept to someone else. Just write enough to remind yourself of the concept. Second, if the mind map process is just not working for you, discard the tool. Instead, take freeform notes on a blank piece of paper. Try to do the important part of the exercise—the thinking about what concepts go together—without letting the tool get in the way.

# **About Building Hands-On Skills**

You need skills in using Cisco routers and switches, specifically the Cisco command-line interface (CLI). The Cisco CLI is a text-based command-and-response user interface; you type a command, and the device (a router or switch) displays messages in response. To answer sim and simlet questions on the exams, you need to know a lot of commands, and you need to be able to navigate to the right place in the CLI to use those commands.

The best way to master these commands is to use them. Sometime during your initial reading of the first part of this book, you need to decide how you personally plan to build your CLI skills. This next topic discusses your options for getting the tools you need to build CLI skills.

# Overview of Lab Options

To effectively build your hands-on CLI skills, you either need real routers and switches, or at least something that acts like routers and switches. People who are new to Cisco technology often choose from a few options to get those skills.

First, you can use real Cisco routers and switches. You can buy them, new or used, or borrow them at work. You can rent them for a fee. You can even rent virtual Cisco router and switch lab pods from Cisco, in an offering called Cisco Learning Labs.

Simulators provide another option. Router and switch simulators are software products that mimic the behavior of the Cisco CLI, generally for the purpose of allowing people to learn. These products have an added advantage when learning: They usually have lab exercises as well.

Simulators come in many shapes and sizes, but the publisher sells simulators that are designed to help you with CCENT and CCNA study—plus they match this book! The Pearson CCENT Network Simulator and the Pearson CCNA Network Simulator both provide an excellent environment to practice the commands, as well as hundreds of focused labs to help you learn what you need to know for the exams. Both products have the same software code base; the CCNA product simply has labs for both ICND1 and ICND2, whereas the CCENT product has only the ICND1 labs.

This book does not tell you what option to use, but you should plan on getting some hands-on practice somehow. The important thing to know is that most people need to practice using the Cisco CLI to be ready to pass these exams.

I (Wendell) have collected some information and opinions about this decision on my website, at http://certskills.com/labgear. Those pages link to sites for Dynamips and for the Pearson simulator. Also, because the information never seemed to exist in any one place, this website includes many details about how to build a CCNA lab using used real Cisco routers and switches.

#### A Quick Start with Pearson Network Simulator Lite

The decision of how to get hands-on skills can be a little scary at first. The good news: You have a free and simple first step. Install the Pearson NetSim Lite that comes with this book.

This lite version of the best-selling CCNA Network Simulator from Pearson provides you with a means, right now, to experience the Cisco CLI. No need to go buy real gear or buy a full simulator to start learning the CLI. Just install it from the DVD in the back of this book.

Of course, one reason that NetSim Lite comes on the DVD is that the publisher hopes you will buy the full product. However, even if you do not use the full product, you can still learn from the labs that come with NetSim Lite while deciding about what options to pursue.

**NOTE** The ICND1 and ICND2 books each contain a different version of the Sim Lite product, each with labs that match the book content. If you bought both books, make sure you install both Sim Lite products.

# For More Information

If you have any comments about the book, submit them via http://www.ciscopress.com. Just go to the website, select Contact Us, and type your message.

Cisco might make changes that affect the CCNA certification from time to time. You should always check http://www.cisco.com/go/ccna and http://www.cisco.com/go/ccent for the latest details.

The Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Academic Edition helps you attain CCNA Routing and Switching certification. This is the CCNA ICND2 certification book from the only Cisco-authorized publisher. We at Cisco Press believe that this book certainly can help you achieve CCNA certification, but the real work is up to you! I trust that your time will be well spent.



# Chapter 5

# **Troubleshooting IPv4 Routing Part II**

Chapter 4, "Troubleshooting IPv4 Routing Part I," began the discussion of IPv4 troubleshooting, looking at the usual first steps when troubleshooting a problem. This chapter moves on to a later stage, when the problem has been isolated to a smaller part of the network, and to a smaller set of possible causes of the problem. The topics in this chapter get specific and look for those root causes: the causes of network problems that have specific solutions that, once a change is made, will solve the original problem.

This chapter breaks down the discussion based on the two major divisions in how packets are forwarded in an IPv4 internetwork. The first half of the chapter focuses on the root causes of problems between a host and its default router. The second half looks at the routers that forward the packet over the rest of a packet's journey, from the router acting as default router all the way to the destination host.

Note that in addition to Chapters 4 and 5, other chapters in this book discuss troubleshooting topics that help when troubleshooting IPv4 internetworks. In particular, Chapter 11, "Troubleshooting IPv4 Routing Protocols," discusses troubleshooting IPv4 routing protocols, namely Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP). Chapter 3, "Troubleshooting LAN Switching," discussed how to troubleshoot LAN issues. Some topics inside the chapters in Part IV explain how to troubleshoot WAN links. Finally, Chapter 16, "Troubleshooting IPv6 Routing," discusses how to apply these same IPv4 troubleshooting concepts to IPv6.

#### This chapter covers the following exam topics:

#### **Troubleshooting**

Identify and correct common network problems

Troubleshoot and resolve interVLAN routing problems

Connectivity

Encapsulation

Subnet

Native VLAN

Port mode trunk status

Troubleshoot and resolve routing issues

routing is enabled

routing table is correct

correct path selection

# **Foundation Topics**

# **Problems Between the Host and the Default Router**

Imagine that you work as a customer support rep (CSR) fielding calls from users about problems. A user left a message stating that he couldn't connect to a server. You could not reach him when you called back, so you did a series of pings from that host's default router, using some of the problem isolation strategies described in Chapter 4. And at the end of those pings, you think the problem exists somewhere between the user's device and the default router—for instance, between router R1 and host A, as shown in Figure 5-1.



Figure 5-1 Focus of the Discussions in This Section of the Chapter

This first major section of the chapter focuses on problems that can occur on hosts, their default routers, and between the two. To begin, this section looks at the host itself, and its four IPv4 settings, as listed in the figure. Following that, the discussion moves to the default router, with focus on the LAN interface, and the settings that must work for the router to serve as a host's default router.

# Root Causes Based on a Host's IPv4 Settings

A typical IPv4 host gets its four key IPv4 settings in one of two ways: either through static configuration or by using DHCP. In both cases, the settings can actually be incorrect. Clearly, any static settings can be set to a wrong number just through human error when typing the values. More surprising is the fact that the DHCP can set the wrong values: The DHCP process can work, but with incorrect values configured at the DHCP server, the host can actually learn some incorrect IPv4 settings.

This section first reviews the settings on the host, and what they should match, followed by a discussion of typical issues.

# Ensure IPv4 Settings Correctly Match

Once an engineer thinks that a problem exists somewhere between a host and its default router, the engineer should review the host's IPv4 settings versus the intended settings. That process begins by guiding the user through the GUI of the host operating system or by using command-line commands native to host operating systems, such as **ipconfig** and **ifconfig**. This process should uncover obvious issues, like completely missing parameters, or if using DHCP, the complete failure of DHCP to learn any of the IPv4 settings.

If the host has all its settings, the next step is to check the values to match them with the rest of the internetwork. The Domain Name System (DNS) server IP address—usually a list of at least two addresses—should match the DNS server addresses actually used in the internetwork. The rest of the settings should be compared to the correct LAN interface on the router that is used as this host's default router. Figure 5-2 collects all the pieces that should match, with some explanation to follow.

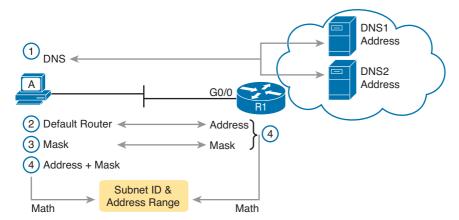


Figure 5-2 Host IPv4 Settings Compared to What the Settings Should Match

As numbered in the figure, these steps should be followed to check the host's IPv4 settings:

- **Step 1.** Check the host's list of DNS server addresses against the actual addresses used by those servers.
- **Step 2.** Check the host's default router setting against the router's LAN interface configuration, for the **ip address** command.
- **Step 3.** Check the subnet mask used by the router and the host; if they use a different mask, the subnets will not exactly match, which will cause problems for some host addresses.
- **Step 4.** The host and router should attach to the exact same subnet—same subnet ID and same range of IP addresses. So, use both the router's and host's IP address and mask, calculate the subnet ID and range of addresses, and confirm they are in the same subnet as the subnet implied by the address/mask of the router's **ip address** command.

If an IPv4 host configuration setting is missing, or simply wrong, checking these settings can quickly uncover the root cause. For instance, if you can log in to the router and do a **show interfaces G0/0** command, and then ask the user to issue an **ipconfig /all** (or similar) command and read the output to you, you can compare all the settings in Figure 5-2.

However, although checking the host settings is indeed very useful, some problems related to hosts are not so easy to spot. The next few topics walk through some example problems to show some symptoms that occur when some of these less obvious problems occur.

#### Mismatched Masks Impact Route to Reach Subnet

A host and its default router should agree about the range of addresses in the subnet. Sometimes, people are tempted to skip over this check, ignoring the mask either on the host or the router and assuming that the mask used on one device must be the same mask as on the other device. However, if the host and router have different subnet mask values, and therefore each calculates a different range of addresses in the subnet, problems happen.

To see one such example, consider the network in Figure 5-3. Host A has IP address/mask 10.1.1.9/24, with default router 10.1.1.150. Some quick math puts 10.1.1.150—the default router address—inside host A's subnet, right? Indeed it does, and it should. Host A's math for this subnet reveals subnet ID 10.1.1.0, with a range of addresses from 10.1.1.1 through 10.1.1.254, and subnet broadcast address 10.1.1.255.

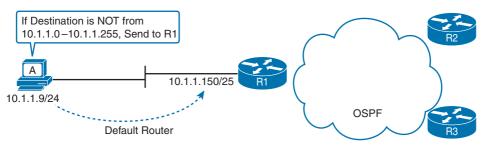


Figure 5-3 Mismatched Subnet Calculations Appear Workable from Host Toward Network

In this case, the host routing of packets, to destinations outside the subnet, works well. However, the reverse direction, from the rest of the network back toward the host, does not. A quick check of router R1's configuration reveals the IP address/mask as shown in Figure 5-3, which results in the connected route for subnet 10.1.1.128/25, as shown in Example 5-1.

**Example 5-1** R1's IP Address, Mask, Plus the Connected Subnet That Omits Host A's Address

```
R1# show running-config interface g0/0
Building configuration...
Current configuration: 185 bytes
interface GigabitEthernet0/0
 description LAN at Site 1
 mac-address 0200.0101.0101
ip address 10.1.1.150 255.255.255.128
 ip helper-address 10.1.2.130
 duplex auto
 speed auto
R1# show ip route connected
! Legend omitted for brevity
      10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
         10.1.1.128/25 is directly connected, GigabitEthernet0/0
L
         10.1.1.150/32 is directly connected, GigabitEthernet0/0
! Other routes omitted for brevity
```

Because of this particular mismatch, R1's view of the subnet puts host A (10.1.1.9) outside R1's view of the subnet (10.1.1.128/25, range 10.1.1.129 to 10.1.1.254). R1 adds a connected route for subnet 10.1.1.128/25 into R1's routing table, and even advertises this route (with OSPF in this case) to the other routers in the network, as seen in Figure 5-4. All the routers know how to route packets to subnet 10.1.1.128/25, but unfortunately, that route does not include host A's 10.1.1.9 IP address.

Hosts should use the same subnet mask as the default router, and the two devices should agree as to what subnet exists on their common LAN. Otherwise, problems may exist immediately, as in this example, or they might not exist until other hosts are added later.

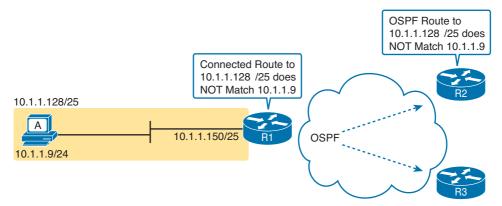


Figure 5-4 Routers Have No Route That Matches Host A's 10.1.1.9 Address

#### Typical Root Causes of DNS Problems

When a host lists the wrong IP addresses for the DNS servers, the symptoms are somewhat obvious: Any user actions that require name resolution fail. Assuming that the only problem is the incorrect DNS setting, any network testing with commands like ping and traceroute fails when using names, but it works when using IP addresses instead of names.

When a ping of another host's hostname fails, but a ping of that same host's IP address works, some problem exists with DNS. For example, imagine a user calls the help desk complaining that he cannot connect to Server1. The CSR issues a ping server1 command from the CSR's own PC, which both works and identifies the IP address of Server1 as 1.1.1.1. Then the CSR asks the user to try two commands from the user's PC: both a ping Server1 command (which fails), and a ping 1.1.1.1 command (which works). Clearly, the DNS name resolution process on the user's PC is having some sort of problem.

This book does not go into much detail about how DNS truly works behind the scenes, but the following two root causes of DNS problems do fit within the scope of the CCENT and CCNA:

- An incorrect DNS server setting
- An IP connectivity problem between the user's host and the DNS server

Although the first problem may be more obvious, note that it can happen both with static settings on the host and with DHCP. If a host lists the wrong DNS server IP address, and the setting is static, just change the setting. If the wrong DNS server address is learned with DHCP, you need to examine the DHCP server configuration. (If using the IOS DHCP server feature, you make this setting with the dns-server server-address command in DHCP pool mode.)

The second bullet point brings up an important issue for troubleshooting any real-world networking problem. Most every real user application uses names, not addresses, and most hosts use DNS to resolve names. So, every connection to a new application involves two sets of packets: packets that flow between the host and the DNS server, and packets that flow between the host and the real server, as shown in Figure 5-5.

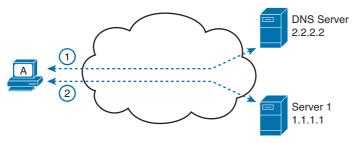


Figure 5-5 DNS Name Resolution Packets Flow First; Then Packets to the Real Server



Finally, before leaving the topic of name resolution, note that the router can be configured with the IP addresses of the DNS servers, so that router commands will attempt to resolve names. For instance, a user of the router command-line interface (CLI) could issue a command ping server1 and rely on a DNS request to resolve server1 into its matching IP address. To configure a router to use a DNS for name resolution, the router needs the ip name-server dns1-address dns2-address... global command. It also needs the ip domain-lookup global command, which is enabled by default.

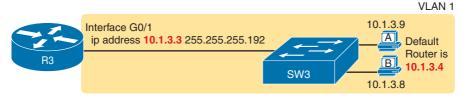
For troubleshooting, it can be helpful to set a router or switch DNS settings to match that of the local hosts. However, note that these settings have no impact on the user DNS requests.

**NOTE** On a practical note, IOS defaults with the **ip domain-lookup** command, but with no DNS IP address known. Most network engineers either add the configuration to point to the DNS servers or disable DNS using the **no ip domain-lookup** command.

#### Wrong Default Router IP Address Setting

Clearly, having a host that lists the wrong IP address as its default router causes problems. Hosts rely on the default router when sending packets to other subnets, and if a host lists the wrong default router setting, the host may not be able to send packets to a different subnet.

Figure 5-6 shows just such an example. In this case, hosts A and B both misconfigure 10.1.3.4 as the default router due to the same piece of bad documentation. Router R3 uses IP address 10.1.3.3. (For the sake of discussion, assume that no other host or router in this subnet currently uses address 10.1.3.4.)



**Figure 5-6** Incorrect Default Router Setting on Hosts A and B

In this case, several functions do work. For instance, hosts A and B can send packets to other hosts on the same LAN. The CSR at the router CLI can issue a ping 10.1.3.9 and ping 10.1.3.8 command, and both work. As a result of those two working pings, R3 would list the MAC address of the two PCs in the output of the show arp command. Similarly, the hosts would list R3's 10.1.3.3 IP address (and matching MAC address) in their ARP caches (usually displayed with the arp –a command). The one big problem in this case happens when the hosts try to send packets off-subnet. In that case, try to send the packets to IP address 10.1.3.4 next, which fails.

# **Root Causes Based on the Default Router's Configuration**

While hosts must have correct IPv4 settings to work properly, having correct settings does not guarantee that a LAN-based host can successfully send a packet to the default router. The LAN between the host and the router must work. In addition, the router itself must be working correctly, based on the design of the internetwork.

This next topic looks at problems between hosts and their default router in which the root cause exists on the router. In particular, this topic looks at three main topics. The first topic looks at the trunking configuration required on a router to support multiple VLANs (known as router on a

stick, or ROAS). Following that, the text examines typical DHCP issues. The final root cause discussed here is the status of the router interface and what causes that interface to fail.

#### Mismatched VLAN Trunking Configuration with Router on a Stick

Examples that teach configuration details often focus on one topic at a time. For instance, IPv4 configuration examples may show a host and its default router setting with the IP address configured on the router's LAN interface, as shown earlier in Example 5-1. However, the details of the LAN to which the host and router attach may be completely omitted, to focus on the IPv4 details.

Troubleshooting, both in real life and on the exams, requires that you put all the pieces together. This next example shows a great case of how the troubleshooting process suffers if you forget to think about both the router and switch part of the problem. This example shows a valid router configuration that, unfortunately, does not match the configuration on the neighboring LAN switch like it should.

The next example focuses on how to connect routers to the subnets on multiple VLANs in the same campus LAN. Today, most sites in an enterprise LAN use at least two VLANs. To make routing work today, one of two options is typically used:

- Router on a Stick (ROAS): A router connects to the LAN, with one physical interface configured for VLAN trunking. The router has an IP address in each subnet, with one subnet per VLAN. The router configuration adds each matched subnet and associated VLAN to a subin-
- Layer 3 switch: Also called a multilayer switch, a Layer 3 switch performs the same job as a router using ROAS, but the switch has routing functions built in. The switch configuration adds each matched subnet and associated VLAN to a VLAN interface.

This example happens to use ROAS, but many of the same kinds of mistakes shown here can be made with Layer 3 switch configurations as well.

First, the following list outlines the rules for configuring ROAS, using 802.1Q, on both the router and the neighboring switch:

- Step 1. On the router, for each VLAN that is not the native VLAN, do the following:
  - **A.** Create a unique subinterface for each VLAN that needs to be routed (interface type number.subint).
  - **B.** Enable 802.1Q, and associate one specific VLAN with the subinterface in subinterface config mode (encapsulation dot1q vlan-id).
  - **C.** Configure IP settings (address and mask) in subinterface config mode (ip address address mask).
- Step 2. On the router, for the native VLAN, if using it, use one of the two following options:
  - **A.** Configure just like for other VLANs, except add the native keyword to the encapsulation command (encapsulation dot1q vlan-id native).

Or

**B.** Configure the IP address on the physical LAN interface, without a subinterface and without the encapsulation dot1q command.



- **Step 3.** On the switch, enable trunking (because the router will not negotiate to enable 802.1Q trunking):
  - **A.** Enable trunking with the **switchport mode trunk** interface subcommand.
  - **B.** Set the native VLAN to the same VLAN expected on the router, using the switchport trunk native vlan *vlan-id* interface subcommand.

Keeping that long list handy for reference, let's next walk through a brief example of the router configuration. First, imagine that previously a site used a single VLAN; so, the router configuration ignored VLAN trunking, with the IP address configured on the physical LAN interface on the router. All hosts sat in default VLAN 1. The router could ignore the VLAN details, not use trunking, and act as default router for all hosts in VLAN 1, as shown in Figure 5-7.

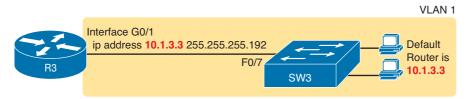


Figure 5-7 Router IP Address Configuration, Without Trunking

Then, management planned an expansion in which a second VLAN will be used. This particular company has one network engineer in charge of routers and the other in charge of switches. When planning the changes with the switch engineer, the two engineers did not listen to each other very well, and then the router engineer went off to plan the changes to the router. The router engineer planned to make the following changes to use ROAS:

- Use ROAS on interface G0/1 to support both users in old subnet 10.1.3.0/26, in VLAN 1, and users in new subnet 10.1.3.64/26, in VLAN 2.
- To support VLAN 1 users, leave 10.1.3.3/26 configured as is on the physical interface. This takes advantage of the option to configure the native VLAN IP address on the physical interface because VLAN 1 is the default native VLAN.
- Add a ROAS subinterface to the router configuration to support VLAN 2, using address 10.1.3.65/26 as the router IP address/mask in that subnet.

Figure 5-8 shows the concepts and configuration.

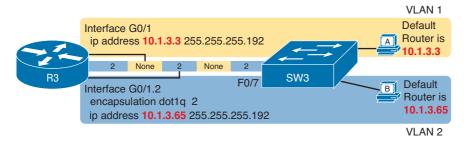


Figure 5-8 Router IP Address Configuration, with ROAS, and Native VLAN 1

This configuration could work perfectly well—as long as the switch has a matching correct VLAN trunking configuration. The router configuration implies a couple of things about VLAN trunking, as follows:

- With the IP address listed on physical interface G0/1, the configuration implies that the router intends to use the native VLAN, sending and receiving untagged frames.
- The router intends to use VLAN 2 as a normal VLAN, sending and receiving frames tagged as VLAN 2.

The switch (SW3) needs to configure VLAN trunking to match that logic. In this case, that means to enable trunking on that link, support VLANs 1 and 2, and make sure VLAN 1 is the native VLAN. Instead, in this case, the switch engineer actually added the trunk configuration to the wrong port, with the F0/7 port, connected to router R3, having these settings:

switchport mode access—The port does not trunk.

switchport access vlan 7—The port is assigned to VLAN 7.

The first command confirms, without a doubt, that the link from R3 to SW3 does not trunk. SW3 will not pass any VLAN 2 traffic over that link at all. A standard ping of host B's IP address from R3 fails; likewise, a ping 10.1.3.65 command from host B fails.

The second command states that the access VLAN on F0/7 is VLAN 7, which means that SW3 will not forward VLAN 1's traffic over the link to R3, either. Again, pings between R3 and hosts in VLAN 1 will fail as well.

In summary, for ROAS configurations, take the time to verify the matching configuration on the neighboring switch. In particular

- Make sure the switch enables trunking (switchport mode trunk).
- Make sure the switch sets the correct VLAN as that trunk's native VLAN (switchport trunk native vlan *vlan-id*).
- Make sure the switch knows about all the VLANs the router has configured (vlan vlan-id).

#### **DHCP Relay Issues**

Hosts that use DHCP to lease an IP address (and learn other settings) rely on the network to pass the DHCP messages. In particular, if the internetwork uses a centralized DHCP server, with many remote LAN subnets using the DHCP server, the routers have to enable a feature called *DHCP Relay* to make DHCP work. Without DHCP Relay, DHCP requests from hosts never leave the local LAN subnet.

Figure 5-9 shows the big ideas behind how DHCP Relay works. In this example, a DHCP client (Host A) sits on the left, with the DHCP server (172.16.2.11) on the right. The client begins the DHCP lease process by sending a DHCP Discover message, one that would flow only across the local LAN without DHCP Relay configured on router R1. To be ready to forward the Discover message, R1 enables DHCP Relay with the **ip helper-address 172.16.2.11** command configured under its G0/0 interface.

The steps in the figure point out the need for DHCP Relay. At Step 1, host A sends a message, with destination IP and L2 broadcast address of 255.255.255.255.255 and ff:ff:ff:ff:ff.ff, respectively. Packets sent to this IP address, the "local subnet broadcast address," should never be forwarded past the router. All devices on the subnet receive and process the frame. Additionally, because of the **ip helper-address** command configured on R1, router R1 will continue to deencapsulate the frame and packet to identify that it is a DHCP request and take action. Step 2 shows the results of DHCP Relay, where R1 changes both the source and destination IP address, with R1 routing the packet to the address listed in the command: 172.16.2.11.

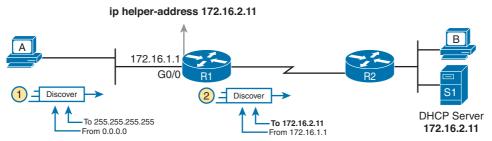


Figure 5-9 IP Helper Address Effect



Now, back to troubleshooting. Messages sent by a DHCP client can reach the DHCP server if the following are true:



- The server is in the same subnet as the client, with connectivity working between the two.
- The server is on another subnet, with the router on the same subnet as the client correctly implementing DHCP Relay, and with IP connectivity from that router to the DHCP server.

Two common mistakes can be made with DHCP Relay, both of which are fairly obvious. If the router omits the **ip helper-address** command on a LAN interface (or subinterface when using ROAS, or VLAN interface with a multilayer switching [MLS] configuration), DHCP fails for those clients. If the configuration includes the **ip helper-address** command but lists the wrong DHCP server IP address, again DHCP fails completely.

The symptom in both cases is that the client learns nothing with DHCP.

For instance, Example 5-2 shows an updated configuration for ROAS on router R3, based on the same scenario as in Figure 5-8. The router configuration works fine for supporting IPv4 and making the router reachable. However, only one subinterface happens to list an ip helper-address command.

**Example 5-2** Forgetting to Support DHCP Relay on a ROAS Subinterface

```
interface GigabitEthernet0/1
ip address 10.1.3.3 255.255.255.192
ip helper-address 10.1.2.130
!
interface GigabitEthernet0/1.2
encapsulation dot1q 2
ip address 10.1.3.65 255.255.255.192
```

In this case, hosts in VLAN 1 that want to use DHCP can, assuming the host at address 10.1.2.130 is indeed the DHCP server. However, hosts in VLAN 2 will fail to learn settings with DHCP because of the lack of an **ip helper-address** command.

#### Router LAN Interface and LAN Issues

At some point, the problem isolation process may show that a host cannot ping its default router and vice versa. That is, neither device can send an IP packet to the other device on the same subnet. This basic test tells the engineer that the router, host, and LAN between them, for whatever reasons, cannot pass the packet encapsulated in an Ethernet frame between the two devices.

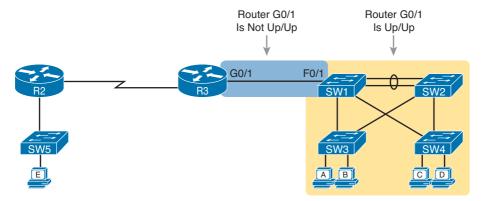
The root causes for this basic LAN connectivity issue fall into two categories:

- Problems that cause the router LAN interface to fail
- Problems with the LAN itself

A router's LAN interface must be in a working state before the router will attempt to send packets out that interface (or receive packets in that interface). Specifically, the router LAN interface must be in an up/up state; if in any other state, the router will not use the interface for packet forwarding. So, if a ping from the router to a LAN host fails (or vice versa), check the interface status, and if not up, find the root cause for the router interface to not be up.

Alternatively, the router interface can be in an up/up state, but problems can exist in the LAN itself. In this case, every topic related to Ethernet LANs may be a root cause. In particular, all the topics reviewed in Chapter 3, such as Ethernet cable pinouts, port security, and even Spanning Tree Protocol, may be root causes of LAN issues.

For instance, in Figure 5-10, router R3 connects to a LAN with four switches. R3's LAN interface (G0/1) can reach an up/up state if the link from R3 to SW1 works. However, many other problems could prevent R3 from successfully sending an IP packet, encapsulated in an Ethernet frame, to the hosts attached to switches SW3 and SW4.



Where to Look for Problems Based on Router LAN Interface Status

**NOTE** This book leaves the discussion of LAN issues, as shown on the right side of Figure 5-10, to Part I of this book.

Router LAN interfaces can fail to reach a working up/up state for several reasons. Table 5-1 lists the common reasons discussed within the scope of the CCNA exam.



Table 5-1 Common Reasons Why Router LAN Interfaces Are Not Up/Up

Reason	Description	Router Interface State
Speed mismatch	The router and switch can both use the <b>speed</b> interface subcommand to set the speed, but to different speeds.	down/down
Shutdown	The router interface has been configured with the <b>shutdown</b> interface subcommand.	Admin down/down
Err-disabled switch	The neighboring switch port uses port security, which has put the port in an err-disabled state.	down/down
No cable/bad are incorrect.*  The router has no cable installed, or the cable pine are incorrect.*		down/down

<sup>\*</sup> Cisco switches use a feature called auto-mdix, which automatically detects some incorrect cabling pinouts and internally changes the pin logic to allow the cable to be used. As a result, not all incorrect cable pinouts result in an interface failing.

Using the speed mismatch root cause as an example, you could configure Figure 5-10's R3's G0/1 with the speed 1000 command and SW1's F0/1 interface with the speed 100 command. The link simply cannot work at these different speeds, so the router and switch interfaces both fall to a down/down state. Example 5-3 shows the resulting state, this time with the show interfaces **description** command, which lists one line of output per interface.

R3# show interfaces description Interface Protocol Description Status Gi0/0 up Gi0/1 down down link to campus LAN Se0/0/0 admin down down Se0/0/1 uρ up Se0/1/0 up admin down Se0/1/1 down

**Example 5-3** show interfaces description Command with Speed Mismatch

# **Problems with Routing Packets Between Routers**

The first half of this chapter focused on the first hop that an IPv4 packet takes when passing over a network. This second major section now looks at issues related to how routers forward the packet from the default router to the final host.

In particular, this section begins by looking at the IP routing logic inside a single router. These topics review how to understand what a router currently does. Following that, the discussion expands to look at some common root causes of routing problems, causes that come from incorrect IP addressing, particularly when the addressing design uses variable-length subnet masks (VLSM).

The end of this section turns away from the core IP forwarding logic, looking at other issues that impact packet forwarding, including issues related to router interface status (which needs to be up/up) and how IPv4 access control lists (ACL) can filter IPv4 traffic.

# IP Forwarding by Matching the Most Specific Route

Any router's IP routing process requires that the router compare the destination IP address of each packet with the existing contents of that router's IP routing table. Often, only one route matches a particular destination address. However, in some cases, a particular destination address matches more than one of the router's routes.

The following CCENT and CCNA features can create overlapping subnets:

- Autosummary (as discussed in Chapter 10, "Implementing EIGRP for IPv4")
- Manual route summarization
- Static routes
- Incorrectly designed subnetting plans that cause subnets to overlap their address ranges

In some cases, overlapping routes cause a problem; in other cases, the overlapping routes are just a normal result of using some feature. This section focuses on how a router chooses which of the overlapping routes to use, for now ignoring whether the overlapping routes are a problem. The section "Routing Problems Caused by Incorrect Addressing Plans," later in this chapter, discusses some of the problem cases.

Now on to how a router matches the routing table, even with overlapping routes in its routing table. If only one route matches a given packet, the router uses that one route. However, when more than one route matches a packet's destination address, the router uses the "best" route, defined as follows:

When a particular destination IP address matches more than one route in a router's IPv4 routing table, the router uses the most specific route—in other words, the route with the longest prefix length mask.

#### Using **show ip route** and Subnet Math to Find the Best Route

We humans have a couple of ways to figure out what choice a router makes for choosing the best route. One way uses the show ip route command, plus some subnetting math, to decide the route the router will choose. To let you see how to use this option, Example 5-4 shows a series of overlapping routes.

**Example 5-4** show ip route Command with Overlapping Routes

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is 172.16.25.129 to network 0.0.0.0
    172.16.0.0/16 is variably subnetted, 9 subnets, 5 masks
       172.16.1.1/32 [110/50] via 172.16.25.2, 00:00:04, Serial0/1/1
       172.16.1.0/24 [110/100] via 172.16.25.129, 00:00:09, Serial0/1/0
       172.16.0.0/22 [110/65] via 172.16.25.2, 00:00:04, Serial0/1/1
       172.16.0.0/16 [110/65] via 172.16.25.129, 00:00:09, Serial0/1/0
0
       0.0.0.0/0 [110/129] via 172.16.25.129, 00:00:09, Serial0/1/0
1
```

**NOTE** As an aside, the show ip route ospf command lists only OSPF-learned routes, but the statistics for numbers of subnets and masks (9 and 5 in the example, respectively) are for all routes, not just OSPF-learned routes.

To predict which of its routes a router will match, two pieces of information are required: the destination IP address of the packet and the contents of the router's routing table. The subnet ID and mask listed for a route define the range of addresses matched by that route. With a little subnetting math, a network engineer can find the range of addresses matched by each route. For instance, Table 5-2 lists the five subnets listed in Example 5-4 and the address ranges implied by each.

Table 5-2 Analysis of Address Ranges for the Subnets in Example 5-4

Subnet/Prefix	Address Range	
172.16.1.1/32	172.16.1.1 (just this one address)	
172.16.1.0/24	172.16.1.0–172.16.1.255	
172.16.0.0/22	172.16.0.0–172.16.3.255	
172.16.0.0/16	172.16.0.0–172.16.255.255	
0.0.0.0/0	0.0.0.0–255.255.255.255 (all addresses)	

#### **NOTE** The route listed as 0.0.0.0/0 is the default route.

As you can see from these ranges, several of the routes' address ranges overlap. When matching more than one route, the route with the longer prefix length is used. That is, a route with /16 is better than a route with /10; a route with a /25 prefix is better than a route with a /20 prefix; and so on.

For example, a packet sent to 172.16.1.1 actually matches all five routes listed in the routing table in Example 5-4. The various prefix lengths range from /0 to /32. The longest prefix (largest /P value, meaning the best and most specific route) is /32. So, a packet sent to 172.16.1.1 uses the route to 172.16.1.1/32, and not the other routes.

The following list gives some examples of destination IP addresses. For each address, the list describes the routes from Table 5-2 that the router would match, and which specific route the router would use.

- 172.16.1.1: Matches all five routes; the longest prefix is /32, the route to 172.16.1.1/32.
- 172.16.1.2: Matches last four routes; the longest prefix is /24, the route to 172.16.1.0/24.
- 172.16.2.3: Matches last three routes; the longest prefix is /22, the route to 172.16.0.0/22.
- 172.16.4.3: Matches the last two routes; the longest prefix is /16, the route to 172.16.0.0/16.

#### Using **show ip route** address to Find the Best Route

A second way to identify the route a router will use, one that does not require any subnetting math, is the show ip route address command. The last parameter on this command is the IP address of an assumed IP packet. The router replies by listing the route it would use to route a packet sent to that address.

For example, Example 5-5 lists the output of the show ip route 172.16.4.3 command on the same router used in Example 5-4. The first line of (highlighted) output lists the matched route: the route to 172.16.0.0/16. The rest of the output lists the details of that particular route, like the outgoing interface of S0/1/0 and the next-hop router of 172.16.25.129.

#### **Example 5-5** show ip route Command with Overlapping Routes

```
R1# show ip route 172.16.4.3
Routing entry for 172.16.0.0/16
 Known via "ospf 1", distance 110, metric 65, type intra area
 Last update from 10.2.2.5 on Serial0/1/0, 14:22:06 ago
 Routing Descriptor Blocks:
 * 172.16.25.129, from 172.16.25.129, 14:22:05 ago, via Serial0/1/0
      Route metric is 65, traffic share count is 1
```

Certainly, if you have an option, just using a command to check what the router actually chooses is a much quicker option than doing the subnetting math.

#### show ip route Reference

The show ip route command plays a huge role in troubleshooting IP routing and IP routing protocol problems. Many chapters in this book and in the ICND1 book mention various facts about this command. This section pulls the concepts together in one place for easier reference and study.

Figure 5-11 shows the output of a sample show ip route command. The figure numbers various parts of the command output for easier reference, with Table 5-3 describing the output noted by each number.

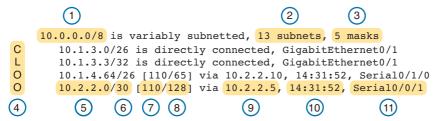


Figure 5-11 show ip route Command Output Reference

Table 5-3 Descriptions of the show ip route Command Output

Item	Idea	Value in the Figure	Description	
1	Classful network	10.0.0.0/8	The routing table is organized by classful network. This line is the heading line for classful network 10.0.0.0; it lists the default mask for class A networks (/8).	
2	Number of subnets	13 subnets	Lists the number of routes for subnets of the classful network known to this router, from all sources, including local routes—the /32 routes that match each router interface IP address.	
3	Number of masks	5 masks	The number of different masks used in all routes known to this router inside this classful network.	
4	Legend code	C, L, O	A short code that identifies the source of the routing information. <i>O</i> is for OSPF, <i>D</i> for EIGRP, <i>C</i> for Connected, <i>S</i> for Static, and <i>L</i> for Local. (See Example 5-4 for a sample of the legend.)	
5	Subnet ID	10.2.2.0	The subnet number of this particular route.	
6	Prefix length	/30	The prefix mask used with this subnet.	
7	Administrative distance	110	If a router learns routes for the listed subnet from more than one source of routing information, the router uses the source with the lowest AD.	
8	Metric	128	The metric for this route.	
9	Next-hop router	10.2.2.5	For packets matching this route, the IP address of the next router to which the packet should be forwarded.	
10	Timer	14:31:52	For OSPF and EIGRP routes, this is the time since the route was first learned.	
11	Outgoing interface	Serial0/0/1	For packets matching this route, the interface out which the packet should be forwarded.	

# **Routing Problems Caused by Incorrect Addressing Plans**

The existence of overlapping routes in a router's routing table does not necessarily mean a problem exists. Both automatic and manual route summarization result in overlapping routes on some routers, with those overlaps not causing problems. However, some overlaps, particularly those related to addressing mistakes, can cause problems for user traffic. So, when troubleshooting, if

overlapping routes exist, the engineer should also look for the specific reasons for overlaps that actually cause a problem.

Simple mistakes in either the IP addressing plan or the implementation of that plan can cause overlaps that also cause problems. In these cases, one router claims to be connected to a subnet with one address range, while another router claims to be connected to another subnet with an overlapping range, breaking IP addressing rules. The symptoms are that the routers sometimes forward the packets to the right host, but sometimes not.

This problem can occur whether or not VLSM is used. However, the problem is much harder to find when VLSM is used. This section reviews VLSM, shows examples of the problem both with and without VLSM, and discusses the configuration and verification commands related to these problems.

# Recognizing When VLSM Is Used or Not

An internetwork is considered to be using VLSM when multiple subnet masks are used for different subnets of *a single classful network*. For example, if in one internetwork all subnets come from network 10.0.0.0, and masks /24, /26, and /30 are used, the internetwork uses VLSM.

Sometimes people fall into the trap of thinking that any internetwork that uses more than one mask must be using VLSM, but that is not always the case. For instance, if an internetwork uses subnets of network 10.0.0.0, all of which use mask 255.255.240.0, and subnets of network 172.16.0.0, all of which use a 255.255.255.0 mask, the design does not use VLSM. Two different masks are used, but only one mask is used in any single classful network. The design must use more than one mask for subnets of a single classful network to be using VLSM.

Only classless routing protocols can support VLSM. The current CCENT and CCNA Routing and Switching certifications cover only classless routing protocols (OSPF and EIGRP), so in all routing protocol discussions for this book, VLSM should be supported. However, for real life, note that RIPv2 (as a classless routing protocol) also supports VLSM, whereas classful routing protocols RIPv1 and Interior Gateway Routing Protocol (IGRP) cannot.

#### Overlaps When Not Using VLSM

Even when you are not using VLSM, addressing mistakes that create overlapping subnets can occur. For instance, Figure 5-12 shows a sample network with router LAN IP address/mask information. An overlap exists, but it might not be obvious at first glance.

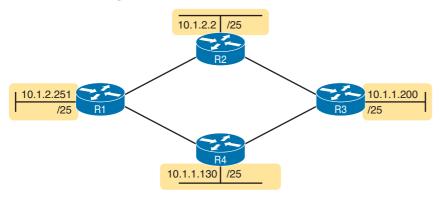


Figure 5-12 IP Addresses on LAN Interfaces, with One Mask (/25) in Network 10.0.0.0

If an overlap exists when all subnets use the same mask, the overlapping subnets have the exact same subnet ID, and the exact same range of IP addresses in the subnet. To find the overlap, all you have to do is calculate the subnet ID of each subnet and compare the numbers. For instance,

Figure 5-13 shows an updated version of Figure 5-12, with subnet IDs shown and with identical subnet IDs for the LANs off R3 and R4.

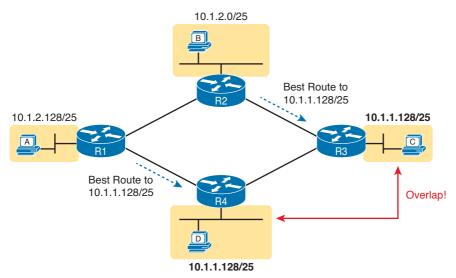


Figure 5-13 Subnet IDs Calculated from Figure 5-12

Using the same subnet in two different places (as is done in Figure 5-13) breaks the rules of IPv4 addressing because the routers get confused about where to send packets. In this case, for packets sent to subnet 10.1.1.128/25, some routers send packets so they arrive at R3, whereas others think the best route points toward R4. Assuming all routers use a routing protocol, such as OSPF, both R3 and R4 advertise a route for 10.1.1.128/25.

In this case, R1 and R2 will likely send packets to two different instances of subnet 10.1.1.128/25. With these routes, hosts near R1 will be able to communicate with 10.1.1.128/25 hosts off R4's LAN, but not those off R3's LAN, and vice versa.

Finally, although the symptoms point to some kind of routing issues, the root cause is an invalid IP addressing plan. No IP addressing plan should use the same subnet on two different LANs, as was done in this case. The solution: Change R3 or R4 to use a different, nonoverlapping subnet on its LAN interface.

#### Overlaps When Using VLSM

When using VLSM, the same kinds of addressing mistakes can lead to overlapping subnets; they just may be more difficult to notice.

First, overlaps between subnets that have different masks will cause only a partial overlap. That is, two overlapping subnets will have different sizes and possibly different subnet IDs. The overlap occurs between all the addresses of the smaller subnet, but with only part of the larger subnet. Second, the problems between hosts only occur for some destinations (specifically the subset of addresses in the overlapped ranges), making it even tougher to characterize the problem.

For instance, Figure 5-14 shows an example with a VLSM overlap. The figure shows only the IP address/mask pairs of router and host interfaces. First, look at the example and try to find the overlap by looking at the IP addresses.

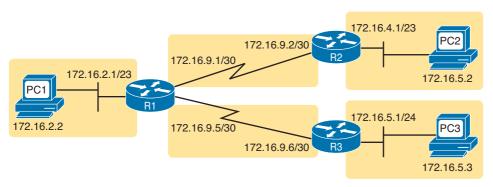


Figure 5-14 VLSM IP Addressing Plan in Network 172.16.0.0

To find the overlap, the person troubleshooting the problem needs to analyze each subnet, finding not only the subnet ID but also the subnet broadcast address and the range of addresses in the subnet. If the analysis stops with just looking at the subnet ID, the overlap may not be noticed (as is the case in this example).

Figure 5-15 shows the beginning analysis of each subnet, with only the subnet ID listed. Note that the two overlapping subnets have different subnet IDs, but the lower-right subnet (172.16.5.0/24) completely overlaps with part of the upper-right subnet (172.16.4.0/23). (Subnet 172.16.4.0/23 has a subnet broadcast address of 172.16.5.255, and subnet 172.16.5.0/24 has a subnet broadcast address of 172.16.5.255.)

To be clear, the design with actual subnets whose address ranges overlap is incorrect and should be changed. However, once implemented, the symptoms show up as routing problems, like the similar case without VLSM. **ping** commands fail, and **traceroute** commands do complete for only certain hosts (but not all).

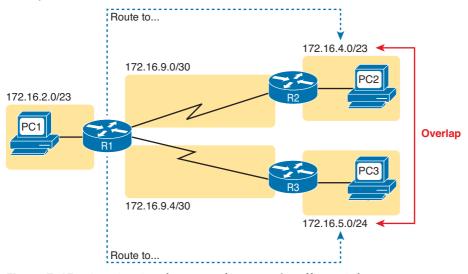


Figure 5-15 A VLSM Overlap Example, But with Different Subnet IDs

#### Configuring Overlapping VLSM Subnets

IP subnetting rules require that the address ranges in the subnets used in an internetwork should not overlap. IOS sometimes can recognize when a new **ip address** command creates an overlapping subnet, but sometimes not, as follows:

■ Preventing the overlap on a single router: IOS detects the overlap when the ip address command implies an overlap with another ip address command *on the same router*.



■ Allowing the overlap on different routers: IOS cannot detect an overlap when an ip address command overlaps with an ip address command on another router.

The router shown in Example 5-6 prevents the configuration of an overlapping VLSM subnet. The example shows router R3 configuring Fa0/0 with IP address 172.16.5.1/24 and attempting to configure Fa0/1 with 172.16.5.193/26. The ranges of addresses in each subnet are as follows:

```
Subnet 172.16.5.0/24: 172.16.5.1 - 172.16.5.254
Subnet 172.16.5.192/26: 172.16.5.193 - 172.16.5.254
```

# **Example 5-6** Single Router Rejects Overlapped Subnets

```
R3# configure terminal
R3(config)# interface Fa0/0
R3(config-if)# ip address 172.16.5.1 255.255.255.0
R3(config-if)# interface Fa0/1
R3(config-if)# ip address 172.16.5.193 255.255.255.192
% 172.16.5.192 overlaps with FastEthernet0/0
R3(config-if)#
```

IOS knows that it is illegal to overlap the ranges of addresses implied by a subnet. In this case, because both subnets would be connected subnets, this single router knows that these two subnets should not coexist because that would break subnetting rules, so IOS rejects the second command.

As an aside of how IOS handles these errors, IOS only performs the subnet overlap check for interfaces that are not in a shutdown state. When configuring an interface in shutdown state, IOS actually accepts the ip address command that would cause the overlap. Later, when the no shutdown command is issued, IOS checks for the subnet overlap and issues the same error message shown in Example 5-6. IOS leaves the interface in the shutdown state until the overlap condition has been resolved.

IOS cannot detect the configuration of overlapping subnets on different routers, as shown in Example 5-7. The example shows the configuration of the two overlapping subnets on R2 and R3 from Figure 5-15.

**Example 5-7** Two Routers Accept Overlapped Subnets

```
! First, on router R2
R2# configure terminal
R2(config)# interface G0/0
R2(config-if)# ip address 172.16.4.1 255.255.254.0
! Next, on router R3
R3# configure terminal
R3(config)# interface G0/0
R3(config-if)# ip address 172.16.5.1 255.255.255.0
```

#### **Router WAN Interface Status**

One of the steps in the IP routing troubleshooting process described earlier, in the "Router LAN Interface and LAN Issues" section, says to check the interface status, ensuring that the required interface is working. For a router interface to be working, the two interface status codes must both be listed as up, with engineers usually saying the interface is "up and up."

So far, the ICND1 and ICND2 books have explored only basic information about how serial links work. For now, know that both routers must have working serial interfaces in an up/up state before they can send IPv4 packets to each other. The two routers should also have serial IP addresses in the same subnet.

Later, the chapters in Part IV further develop the details of WAN links, including what is required for routers to use these links to forward IP packets.

# Filtering Packets with Access Lists

Access control lists (ACL) cause some of the biggest challenges when troubleshooting problems in real networking jobs. End-user packets sent by user applications do not look exactly like packets sent by testing tools such as ping and traceroute. The ACLs sometimes filter the ping and traceroute traffic, making the network engineer think some other kind of problems exists when no problems exist at all. Or, the problem with the end-user traffic really is caused by the ACL, but the ping and traceroute traffic works fine, because the ACL filters the user traffic but not the ping and traceroute traffic.

This section summarizes some tips for attacking ACL-related problems in real life and on the exams:

- Step 1. Determine on which interfaces ACLs are enabled, and in which direction (show running-config, show ip interfaces).
- Step 2. Determine which ACL statements are matched by test packets (show access-lists, show ip access-lists).
- Step 3. Analyze the ACLs to predict which packets should match the ACL, focusing on the following points:
  - **A.** Remember that the ACL uses first-match logic.
  - **B.** Consider using the (possibly) faster math described in the ICND1 book, Chapter 22, "Basic IP Access Control Lists," to find the range of addresses matched by an ACL command: Add the address and wildcard mask to find the end of the numeric range.
  - **C.** Note the direction of the packet in relation to the server (going to the server, coming from the server). Make sure that the packets have particular values as either the source IP address and port, or as the destination IP address and port, when processed by the ACL enabled for a particular direction (in or out).
  - **D.** Remember that the **tcp** and **udp** keywords must be used if the command needs to check the port numbers.
  - **E.** Note that ICMP packets do not use UDP or TCP. ICMP is considered to be another protocol matchable with the icmp keyword (instead of tcp or udp).
  - **F.** Instead of using the implicit **deny** any at the end of each ACL, use an explicit configuration command to deny all traffic at the end of the ACL so that the show command counters increment when that action is taken.

If you suspect ACLs are causing a problem, the first problem-isolation step is to find the location and direction of the ACLs. The fastest way to do this is to look at the output of the show running-config command and to look for ip access-group commands under each interface. However, in some cases, enable mode access may not be allowed, and show commands are required. In that case, another way to find the interfaces and direction for any IP ACLs is the show ip interfaces command, as shown in Example 5-8.

# **Example 5-8** *Sample* show ip interface *Command*

```
R1>show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
 Internet address is 10.1.2.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.9
Outgoing access list is not set
Inbound access list is 102
! roughly 26 more lines omitted for brevity
```

Note that the command output lists whether an ACL is enabled, in both directions, and which ACL it is. The example shows an abbreviated version of the show ip interface \$0/0/1 command, which lists messages for just this one interface. The show ip interface command would list the same messages for every interface in the router.

Step 2 then says that the contents of the ACL must be found. Again, the quickest way to look at the ACL is to use the show running-config command. If not available, the show access-lists and show ip access-lists commands list the same details shown in the configuration commands and a counter for the number of packets matching each line in the ACL. Example 5-9 shows an example.

#### **Example 5-9** show ip access-lists Command Example

```
R1# show ip access-lists
Extended IP access list 102
   10 permit ip 10.1.2.0 0.0.0.255 10.1.4.0 0.0.1.255 (15 matches)
```

After the locations, directions, and configuration details of the various ACLs have been discovered in Steps 1 and 2, the hard part begins—interpreting what the ACL really does.

Of particular interest is the last item in the troubleshooting tips list, item 3F. In the ACL shown in Example 5-9, some packets (15 so far) have matched the single configured access-list statement in ACL 102. However, some packets have probably been denied because of the implied deny all packets logic at the end of an ACL. If you configure the access-list 102 deny ip any any command at the end of the ACL, which explicitly matches all packets and discards them, the show ip access-lists command would then show the number of packets being denied at the end of the ACL.

Finally, as a reminder about interpreting ACL commands, when you know the command comes from a router, it is easy to decide the range of addresses matched by an address and wildcard mask. The low end of the range is the address (the first number), and the high end of the range is the sum of the address and wildcard mask. For instance, with ACL 102 in Example 5-9, which is obviously configured in some router, the ranges are as follows:

Source 10.1.2.0, wildcard 0.0.0.255: Matches from 10.1.2.0 through 10.1.2.255 Destination 10.1.4.0, wildcard 0.0.1.255: Matches from 10.1.4.0 through 10.1.5.255

### **Review Activities**

## **Chapter Summary**

- Many problems can occur on the host or the default router, or between the two.
- A typical IPv4 host gets its four key IPv4 settings either statically or dynamically.
- To begin troubleshooting the host, use the ipconfig or ifconfig command to ensure IPv4 settings correctly match. If you are using DHCP, the ipconfig or ifconfig command will enable you to see whether DHCP has failed to learn any of the IPv4 settings.
- The host and router should attach to the exact same subnet with the same subnet ID and same range of IP addresses.
- When a host lists the wrong IP addresses for the DNS servers, the user actions that require name resolution will fail.
- Any network testing with commands like ping and traceroute fails when using names but works when using IP addresses when there is a problem with the DNS settings.
- Having a host that lists the wrong IP address as its default router will cause network problems.
- The default router's configuration can cause problems in a network that may stem from mismatched VLAN trunking configurations, DHCP relay issues, router LAN interface, and LAN
- If a router omits the ip helper-address command on a LAN interface, DHCP fails for those clients.
- Another problem with network connectivity can exist with the routing or how a router forwards a packet.
- The show ip route command plays a huge role in troubleshooting IP routing and IP routing protocol problems.
- In some cases, overlapping routes cause a problem, while in other cases, the overlapping routes are just a normal result of using some feature.

# **Review All the Key Topics**

Review the most important topics from this chapter, noted with the Key Topic icon. Table 5-4 lists these key topics and where each is discussed.



Table 5-4 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
List	Two root causes of DNS problems.	136
List	The rules for configuring ROAS.	138
List	Items to verify for switch trunking configuration to match a router's ROAS configuration.	140
List	Conditions that must be true for DHCP messages to be able to flow from a client to a DHCP server.	141
Table 5-1	Common reasons why router LAN interfaces are not up/up.	142
Definition	When more than one route matches a packet's destination address, the router uses the "best" (most specific) route.	143
List	Types of overlapping IP address configuration issues that IOS can and cannot recognize.	149

# **Complete the Tables and Lists from Memory**

Print a copy of DVD Appendix D, "Memory Tables," or at least the section for this chapter, and complete the tables and lists from memory. DVD Appendix E, "Memory Tables Answer Key," includes completed tables and lists to check your work.

# **Definitions of Key Terms**

After your first reading of the chapter, try to define these key terms, but do not be concerned about getting them all correct at that time. Chapter 22 directs you in how to use these terms for late-stage preparation for the exam.

forward route, reverse route





# Index

**Symbols** 

fiers), 342-344

#### Layer 3 addressing, 345-348 unicast IPv6 addresses, 411-413 3DES (Triple DES), 180 adjacent OSPFv2 neighbors, 206 3G mobile phone access, 397-398 administrative distance (AD), 215-216 4G mobile phone access, 397-398 ADSL (asymmetric DSL), 395 AES (Advanced Encryption Standard), Α 180 alternate (root) ports, 573-574 ABR (Area Border Router), 208 anti-replay, 177 access control lists (ACLs), 151-152, Area Border Router (ABR), 208 585-588 areas (OSPF) access interface VLAN assignments, design advantages, 209 checking, 92 design rules, 207 access links design terminology, 207-208 AR (access rate), 338 explained, 206-207 Frame Relay, 338 intra-area topology, 210-212 Layer 1 issues, 370 multi-area design, 212-213 Layer 2 issues, 371 multi-area OSPFv2, 217-223 access rate (AR), 338 reducing SPF calculation time with, 208 access VPNs (virtual private networks), 178 single-area OSPF, 206 single-area OSPFv2, 218-21 ACLs (access control lists), 151-152, 585-588 ARP (Address Resolution Protocol), 114 activating IOS software, 529-530 Inverse ARP, 360 Cisco License Manager (CLM), 530-531 replies (unicast), forwarding path of, manual activation, 531-536 98-101 right-to-use licenses, 536-538 requests (broadcast), forwarding path of, 95-98 active/passive model, 160 sample ARP process, 115 active/standby model, 160 ASA (Adaptive Security Appliances), 179 active virtual gateway (AVG), 163 ASN (autonomous system number), 239 active VLANs, checking for, 92-93 AD (administrative distance), 215-216 asymmetric DSL (ADSL), 395 authentication Adaptive Security Appliances (ASA), 179 PAP/CHAP authentication, 328-329 address mapping (Frame Relay) PPP (Point-to-Point Protocol), 322-323 Inverse ARP, 360 authNoPriv security level, 492 static mapping, 360-361 authPriv security level, 492 Address Resolution Protocol. See ARP auto-cost reference-bandwidth addresses command, 225, 228, 440, 458 Frame Relay, 357-359 autonomous system number (ASN), 239 DLCI (data link connection identi-

frame forwarding, 344

### autosummarization bridge ID (BID), 20, 39-40 discontiguous classful networks, 271-272 bridge protocol data units (BPDU), 20-21 example of, 270-271 broadcast storms, 16-17 auto-summary command, 253, 271, 276 broadcasts ARP requests, forwarding path of, 95-98 AVG (active virtual gateway), 163 forwarding in VLAN 3, 97-98 В ignoring, 96-97 backbone area, 208 backbone routers, 208 Cable Internet, 396 backup (designated) ports, 575-576 cable TV (CATV), 396 backup DRs (BDRs), 205, 221-222 balancing load cabling pinouts for LAN switches, 75 EIGRPv4, 267-269 calculating EIGRPv6, 465 powers of 2, 567 HSRP (Hot Standby Router Protocol), 162 routes with EIGRP (Enhanced Interior Gateway Routing Protocol) OSPFv2 (Open Shortest Path First version 2), 225 bandwidth issues, 243 with PSVT+ (Per-VLAN Spanning Tree example, 242-243 Plus), 38 FD (feasible distance), 244-245 bandwidth metric calculation, 241 EIGRPv4 metric calculation, 243 RD (reported distance), 244-245 EIGRPv6 settings, 464-465 CATV (cable TV), 396 reference bandwidth, 225 CCNA practice exams, 552-553 bandwidth command, 224, 228, 243, CDP (Cisco Discovery Protocol), 72-73, 264, 269, 276, 318, 334, 383, 440, 87-88 458, 462, 477 cdp enable command, 73 Basic Rate Interface (BRI), 394 cdp run command, 73 BDR (backup DRs), 205, 221-222 Challenge Handshake Authentication BID (bridge ID), 20, 39-40 Protocol. See CHAP binary-to-hexadecimal conversion, 566 channel-group command, 48-50, 57-58, blocking state (STP), 18-20 boot sequence of Cisco IOS Software, Channel service unit/data service unit. 507-508 See CSU/DSU configuration register, 509 CHAP (Challenge Handshake IOS image verification, 512-513 Authentication Protocol), 398 OS selection process, 509-511 configuring, 324-325 recovery if IOS does not load, 511 troubleshooting, 328-329 three-router operating systems, 508-509 checking boot system command, 509-510, 524 active interface VLAN assignments, 92 boot system flash command, 511, 524 for active VLANs, 92-93 boot system rom command, 524 choosing boot system tftp command, 511 DPs (designated ports), 24-25 BPDU (bridge protocol data units), 20-21 RPs (root ports), 23-24 BPDU Guard, 30-31, 46-47 CIR (committed information rate), 338

BRI (Basic Rate Interface), 394

circuits	load balancing, 267-269
PVC (permanent virtual circuits), 338,	maximum-paths, 267-269
372-377	metric calculation, 269-270
SVC (switched virtual circuits), 338	metric components, 266-267
VC (virtual circuits)	successors, 262-263
explained, 337-340	topology table, viewing, 261-262
Layer 3 addressing, 345-346	variance, 268-269
Cisco Catalyst switches, 80	verifying core features of, 255-260
Cisco Certification Exam Tutorial,	wildcard masks, 255
546-547	EIGRPv6
Cisco Learning Network, 558	bandwidth and delay settings,
Cisco License Manager (CLM), 530-531	464-465
Cisco Prime, 487	basic configuration, 461
Cisco Product License Registration	compared to EIGRPv4, 466-467
Portal, 532	configuration commands, 462
classful routing protocols, 270	example, 462-464
clear ip ospf process command, 202,	interfaces, 467-469
229, 296	IPv6 routes, 472-473
CLI (command-line interface), 556-557	load balancing, 465
clients, VPN (virtual private network)	neighbors, 469-470
clients, 179	overview, 461
CLM (Cisco License Manager), 530-531	timers, 466
clock rate command, 316-318	topology database, 470-472
clock speed command, 334	EtherChannel, 47-48
collector (NetFlow), 500	Channel, 48-49
committed information rate (CIR), 338	channel-group command options,
community strings (SNMP), 490	57-58
config-register command, 509, 524	interface configuration settings,
configuration files, 517-518	58-59
copying, 519-520	manual EtherChannel, 50
erasing, 519-520	Frame Relay
running-config, 517	address mapping, 357-361
setup mode, 521	encapsulation, 356
startup-config, 517	fully meshed networks with one II
configuration register, 509	subnet, 354-355
configuring	LMI (Local Management
BPDU Guard, 46-47	Interface), 356
CHAP (Challenge Handshake	multipoint subinterfaces, 366-368
Authentication Protocol), 324-325	OSPF (Open Shortest Path First), 368-369
Cisco Catalyst switches, 80	
EIGRPv4	planning configurations, 353-354
basic configuration, 253-254	point-to-point subinterfaces, 361-364
compared to EIGRPv6, 466-467	self-assessment, 381-382
convergence, 265-266	verification, 364-365
feasible successors, 263-265	GLBP (Gateway Load Balancing
	Protocol), 167-169
	11000001, 10. 10/

STP (Spanning Tree Protocol)
BID (bridge ID), 39-40
BPDU Guard, 46-47
defaults/configuration options, 40
EtherChannel, 47-50
per-VLAN configuration settings,
38-39
per-VLAN costs, 40
port costs, 44
PortFast, 46-47
STP mode, 37-38
STP port costs, 43-45
switch priority, 44-46
system ID extension, 39-40
verifying STP operation, 40-43
Syslog (System Message Logging),
494-495
confreg command, 514
contiguous classful networks, 271
control plane, 66
control plane analysis, 67-68
convergence
EIGRP (Enhanced Interior Gateway
Routing Protocol)
explained, 244
•
feasible successors, 265-266
query/reply process, 246-247
successors, 245-246
STP (Spanning Tree Protocol), 19
delays, 28
troubleshooting, 56
converting
binary to hexadecimal, 566
decimal to binary, 563-565
hexadecimal to binary, 566
copy command, 519, 525
copy running-config startup-config
command, 509, 515, 519, 525
copy startup-config running-config
command, 515-519, 525
copying
configuration files, 519-520
images into Flash memory, 505-507
CPE (customer premise equipment), 313
CSU/DSU, 315
customer premise equipment (CPE), 313

OSPFv3, 440-441

D	delay, EIGRPv6 settings, 464-465 delay command, 269, 276, 462, 477
data communications equipment (DCE), 338	delivery headers, 184 DES (Data Encryption Standard), 180
Data Encryption Standard (DES), 180	description command, 334
data link connection identifiers (DLCI), 338	designated ports (DPs) choosing, 24-25
explained, 342	determining, 54-55
frame forwarding, 343-344	explained, 19
local DLCI, 342-343	RSTP (Rapid Spanning Tree Protocol),
data link headers, building, 114-115	575-576
data plane, 66	strategies for DP exam questions, 55-56
data plane analysis, 66-67	designated routers (DRs), 205-206
data terminal equipment (DTE), 337-338,	determining
345	duplex issues, 77-78
datak9, 530	root switches, 51-52
Dead Interval timer, 204	RPs (root ports), 52-54
debug eigrp fsm command, 277	switch interface speed, 76-78
debug eigrp packets command, 302	DHCP (Dynamic Host Configuration
debug frame-relay lmi command, 365, 384	Protocol)
debug ip ospf adj command, 294, 302	Relay, 140-141
debug ip ospf events command, 302	stateful DHCP, 424-425
debug ip ospf hello command, 297, 302	stateful DHCPv6, 413-414
debug ip ospf packet command, 302	dial access, 393-394
debug ipv6 ospf adj command, 445	dialer pool command, 400
debug ppp authentication command, 328, 335	Diffusing Update Algorithm (DUAL), 246
debug ppp negotiation command, 335	digital subscriber line (DSL), 395-396
debug spanning-tree events command, 44, 63	dir command, 541 discontiguous classful networks,
decimal-to-binary conversion, 563-565	271-272
dedicated routers (DRs), verifying, 221-222	distance vector (DV) routing protocols explained, 233-234
default-information originate command, 441-442	full update messages, 234-235 route poisoning, 236-237
default routers, troubleshooting, 133	1
DHCP Relay, 140-141	split horizon, 235-236
DNS problems, 136-137	DLCI (data link connection identifiers)
IP address settings, 137	explained, 342
LAN issues, 141-142	frame forwarding, 343-344
	Frame Relay, 338
mismatched IPv4 settings, 133-134	local DLCI, 342-343
mismatched masks, 134-135	DNS (Domain Name Service)
mismatched VLAN trunking configuration, 138-140	name resolution, 123
default routes	troubleshooting
OSPFv2, 591-592	in IPv4, 136-137
031174, 371-374	in IPv6, 424

dns-server command, 136	maximum-paths, 267-269
Domain Name Service. See DNS	variance, 268
DPs (designated ports)	convergence, 265-266
choosing, 24-25	explained, 244
determining, 54-55	query/reply process, 246-247
explained, 19	successors, 245-246, 265
RSTP (Rapid Spanning Tree Protocol),	development of, 231
575-576	discontiguous classful networks,
strategies for DP exam questions, 55-56	271-272
DROthers, 206	DUAL (Diffusing Update Algorithm), 246
DRs (dedicated routers), 221-222	explained, 239
DRs (designated routers), 205-206	feasible successors, 263-265
DSL (digital subscriber line), 395-396	hello packets, 237-238
DSLAM (DSL access multiplexer), 395	interfaces
DTE (data communications equipment),	troubleshooting, 280-286
337-338, 345	working interfaces, 282-284
DUAL (Diffusing Update Algorithm), 246	load balancing, 267-269
duplex half command, 77	loop avoidance, 244
duplex mismatch, 77-78, 89-90	metric calculation, 269-270
duplicate OSPF router IDs, finding,	metric components, 266-267
295-296	neighbors, 239-240
DV (distance vector) routing protocols	troubleshooting, 289-292
explained, 233-234	verification checks, 290-291
full update messages, 234-235	partial update messages, 237
route poisoning, 236-237	route calculation
split horizon, 235-236	bandwidth issues, 243
dynamic EtherChannels, configuring, 50	example, 242-243
_	FD (feasible distance), 244-245
E	metric calculation, 241
	RD (reported distance), 244-245
Echo Requests (ICMP), 127	self-assessment, 248-249, 274-275
edge ports, 576	Split Horizon issues, 595-597
EIGRP router-id command, 258,	successors, 262-263
462-463, 477	topology table, 261-262
EIGRPv4 (Enhanced Interior Gateway	troubleshooting
Routing Protocol version 4), 460 advantages of, 232	interfaces, 280-286
autosummarization	neighbors, 289-292
	overview, 279-280
discontiguous classful networks, 271-272	update messages, 240-241
example of, 270-271	variance, 268-269
compared to EIGRPv6, 466-467	verifying core features of, 255
compared to other routing protocols,	interfaces, 256-258
232-233, 238	IPv4 routing table, 259-260
configuring	neighbor status, 258-259
hasic configuration, 253-254	wildcard masks, 255

feasible successors, 265

dynamic EtherChannel, 50

58-59

interface configuration settings,

manual EtherChannel, 48-49

EIGRPv6 (Enhanced Interior Gateway	troubleshooting, 56
Routing Protocol version 6)	channel-group command options,
bandwidth and delay settings, 464-465	57-58
basic configuration, 461	interface configuration settings, 58-59
compared to EIGRPv4, 466-467	
configuration commands, 462	Ethernet
configuration example, 462-464	emulation, 389
explained, 461	EoMPLS (Ethernet over MPLS), 389
interfaces, 467-469	Ethernet WANs (wide area networks),
IPv6 routes, 472-473	389-390
load balancing, 465	links, designated routers on, 205-206
neighbors, 469-470	PPPoE (PPP over Ethernet)
self-assessment, 475-476	configuring, 399-400
Split Horizon issues, 595-597	explained, 398-399
timers, 466	eui-64 keyword, 416
topology database, 470-472	exam advice
electing root switches via STP (Spanning Tree Protocol), 21-22	Cisco Certification Exam Tutorial, 546-547
emulation, Ethernet, 389	exam-day advice, 548-549
encapsulation	Exam Review
end-to-end, 378	exam-taking tips, 553-554
Frame Relay, 341-342, 356	math-related skills, 549-550
encapsulation command, 138, 318, 334,	practice exams, 551-553
371	hands-on CLI skills, practicing, 556-557
encapsulation frame-relay command,	other study tasks, 558
353-355, 371, 383	pre-exam suggestions, 548
encapsulation hdlc command, 318	Question Review, 554-556
encapsulation ppp command, 323-324	time management, 547-548
encryption	Exam Review
encryption keys, 179	math-related skills, 549-550
IPsec, 179-180	practice exams
end-to-end encapsulation, 378	exams, 551-553
Enhanced Interior Gateway Routing	exam-taking tips, 553-554
Protocol. See EIGRPv4; EIGRPv6	Question Review, 554-556
EoMPLS (Ethernet over MPLS), 389	exchanging LSAs with neighbors, 203-204
equal-cost load balancing, 263	extended ping, 119-121
erase nvram command, 520, 525	extended pmg, 119 121 extended traceroute command, 126-127
erase startup-config command, 520, 525	extranet VPNs (virtual private
erasing configuration files, 519-520	networks), 178
EtherChannel, 29-30	·
configuring, 47-48	F
channel-group command options,	•
57-58	failover, HSRP (Hot Standby Router

Protocol), 161-162

FD (feasible distance), 244-245

FCS (Frame Check Sequence) field, 316

feasible successors (EIGRP), 245-246	LAN switches, 11-12, 71-72
convergence via, 265-266	unicasts, 99-100
creating/viewing, 265	forwarding state (STP), 18-19
finding, 263-265	DPs (designated ports)
FHRP (First Hop Redundancy Protocol)	choosing, 24-25
benefits of, 159-160	explained, 19
comparison of protocols, 590	reasons for, 20
explained, 156-160	root switches
GLBP (Gateway Load Balancing	electing, 21-22
Protocol)	explained, 19
active virtual gateway (AVG), 163	RPs (root ports), 19
configuring, 167-169	Frame Check Sequence (FCS) field, 316
explained, 160, 163-164	Frame Relay, 336-388
verifying, 167-169	access links, 338
HSRP (Hot Standby Router Protocol)	Layer 1 issues, 370
configuring, 164-167	Layer 2 issues, 371
explained, 160-161	addressing, 344
failover, 161-162	AR (access rate), 338
influencing active router choice, 588-589	configuring
load balancing, 162	address mapping, 357-361
verifying, 164-167	encapsulation, 356
need for network redundancy, 157-158	fully meshed networks with one IP
self-assessment, 170-172	subnet, 354-355
single points of failure, 157-158	LMI (Local Management
VRRP (Virtual Router Redundancy	Interface), 356
Protocol), 160	multipoint subinterfaces, 366-368
filtering	OSPF (Open Shortest Path First),
LAN switching, 79-82, 90-91	368-369
packets with ACLs (access control lists),	planning configurations, 353-354
151-152	point-to-point subinterfaces, 361-364
finding	self-assessment, 381-382
duplicate OSPF router IDs, 295-296	verification, 364-365
EIGRPv4 feasible successors, 263-265	DCE (data communications equipment),
EIGRPv4 successors, 262-263	338
Hello/dead timer mismatches, 296-297	DLCI (data link connection identifiers),
First Hop Redundancy Protocol. See	338
FHRP	explained, 342
Flash memory, upgrading IOS software	frame forwarding, 343-344
images into, 505-507	local DLCI, 342-343
floating static routes, 585	DTE (data terminal equipment), 337-338.
flows (network), 497 Forward Delay timers (STP), 26-28	345
- · · · · · · · · · · · · · · · · · · ·	encapsulation and framing, 341-342
forwarding	Layer 3 addressing
forwarding	hybrid approach, 347-348
broadcasts in VLAN 3, 97-98	one subnet per VC (virtual circuit),
IP forwarding, 143-146	345-346

Protocol)

single subnets containing all DTE, gateways, active virtual gateway (AVG), generic routing encapsulation tunnels. LMI (Local Management Interface), See GRE tunnels 337-341 GLBP (Gateway Load Balancing NBMA (nonbroadcast multiaccess) Protocol) networks, 337-338 active virtual gateway (AVG), 163 overview, 337-341 comparing with other FHRPs (First Hop private WANs, 388 Redundancy Protocols), 590 PVC (permanent virtual circuits), 338 configuring, 167-169 subinterface status, 377 explained, 160, 163-164 troubleshooting, 372-377 verifying, 167-169 self-assessment, 349-350 glbp group ip virtual-ip command, 167 SVC (switched virtual circuits), 338 GRE (generic routing encapsulation) troubleshooting, 369 end-to-end encapsulation, 378 configuring, 185-187 Layer 1 issues on access links, 370 explained, 181-182 Layer 2 issues on access links, 371 over unsecured network, 183-184 mapping issues, 377-378 routing over, 182-183 mismatched subnet numbers, 379 tunnel interfaces, 182-184 PVC (permanent virtual circuit) verifying, 187-189 problems, 372-377 self-assessment, 381-382 Н suggested process, 369-370 VC (virtual circuits) HDLC (High-level Data Link Control) explained, 337-340 leased-line WANs Layer 3 addressing, 345-346 building WAN links, 315-316 frame-relay interface-dlci command, CSU/DSU, 315 354-356, 363, 367, 377, 383 explained, 311 frame-relay inverse-arp command, 383 HDLC configuration, 317-320 frame-relay lmi-type ansi command, 356, layer 1 leased lines, 311-316 frame-relay lmi-type command, 341, layer 2 leased lines, 316-317 353, 356, 383 leased line components, 312-314 frame-relay map command, 354, 356, T-carrier system, 314 361, 377, 383 overview, 113 full-mesh Frame Relay networks, 340 Hello/dead timer mismatches, finding, Full neighbor state (OSPF neighbors), 206 296-297 full update messages, 234-235 Hello Interval timer, 204 fully adjacent OSPFv2 neighbors, 206 hello packets (EIGRP), 237-238 fully meshed networks with one IP Hello timers (STP), 26-28 subnet, 354-355 hexadecimal-to-binary conversion, 566 high availability campus network design, 159 High-Level Data Link Control. See HDLC Gateway Load Balancing Protocol. host IPv4 routing logic, 111-112 See GLBP (Gateway Load Balancing

hostname command, 518

hostnames, pinging, 123-124	universal images, 528
hosts	upgrading into Flash memory, 505-507
IPv4 routing, troubleshooting	inferior hello (STP), 21
DNS problems, 136-137	infinity, 236
IP address settings, 137	Integrated Services Digital Network
mismatched IPv4 settings, 133-134	(ISDN), 393-394
mismatched masks, 134-135	interarea routes, 208
IPv6 hosts, configuring	interface loopback command, 229
router address, 415-416	interface serial command, 363, 383
stateful DHCPv6, 413-414	interface status codes for LAN switches, 74-75
stateful SLAAC (stateless address	, . , 0
autoconfiguration), 414-415	interface tracking, 588-589
static routes, 416-417	interface tunnel command, 184-186
verifying connectivity, 417-420	interfaces
Hot Standby Router Protocol. See HSRP	EIGRPv4 interfaces, 595-597
HSRP (Hot Standby Router Protocol)	finding, 256-258
comparing with other FHRPs (First Hop	troubleshooting, 280-286
Redundancy Protocols), 590	EIGRPv6 interfaces, 467-469, 595-597
configuring, 164-167	isolating (LAN switching), 73-78, 88-90
explained, 160-161	cabling pinouts, 75
failover, 161-162	interface status codes, 74-75
influencing active router choice, 588-589	notconnect state, 75
load balancing, 162	OSPFv2 interfaces, 280-281, 286-288
verifying, 164-167	OSPFv3 interfaces
	troubleshooting, 443-444
	verifying, 443
	Internal routers, 208
ICMP (Internet Control Message	Internet Access Links, 392
Protocol), 115, 127	Internet Control Message Protocol (ICMP), 115, 127
ICND2 practice exams, 551-552	Internet Protocol. See IP
identifying STP mode on Catalyst switches, 577-579	intra-area routes, 208
IDs	Inverse ARP, 360
BID (bridge ID), configuring, 39-40	IOS file management
system ID extension, configuring, 39-40	configuration files, 517-518
IEEE 802.1d. See STP (Spanning Tree	copying, 519-520
Protocol)	erasing, 519-520
IEEE 802.1w. See RSTP (Rapid Spanning	running-config, 517
Tree Protocol)	setup mode, 521
ifconfig command, 417, 433	startup-config, 517
IFS (IOS File System), 520	IOS software
ignoring incoming broadcast frame,	boot sequence, 507-508
96-97	configuration register, 509
images (IOS)	IOS image verification, 512-513
images per feature set combination, 528	OS selection process, 509-511
images per model/series, 527	

recovery if IOS does not load, 511 ip flow egress command, 497 three-router operating systems, ip flow-export command, 497 505-509 ip flow-export destination command, password recovery 498 example, 515-517 ip flow-export source command, 498 explained, 513-515 ip flow-export version command, 498 self-assessment, 505, 523-524 ip flow ingress command, 497 IOS File System (IFS), 520 ip hello-interval eigrp command, 253, IOS packaging 301, 462 explained, 527 ip helper-address command, 140-141 images per feature set combination, 528 ip hold-time eigrp command, 253, 276, images per model/series, 527 301, 462 universal images, 528 ip mtu command, 450 IOS software activation, 529-530 ip name-server command, 137 boot sequence, 507-508 ip ospf cost command, 223-225, 228, configuration register, 509 IOS image verification, 512-513 ip ospf dead-interval command, 301 OS selection process, 509-511 ip ospf hello-interval command, 301 recovery if IOS does not load, 511 ip ospf network point-to-multipoint three-router operating systems, command, 368 508-509 ip ospf subcommand, 592-593 Cisco License Manager (CLM), 530-531 ip route command, 215, 582-584 images, upgrading into Flash memory, ip split-horizon eigrp asn command, 596 505-507 ipbasek9, 530 manual activation ipconfig command, 417, 433 activation process, 531-533 IPCP (IP Control Protocol), 321 adding permanent technology IPsec VPNs (virtual private networks), package license, 535-536 179-180 showing current license status, IPv4 routing 533-534 default router IP address settings, 137 right-to-use licenses, 536-538 delivery headers, 184 self-assessment, 540 DV (distance vector) routing protocols IP (Internet Protocol) explained, 233-234 default router IP address settings full update messages, 234-235 troubleshooting, 137 route poisoning, 236-237 delivery headers, 184 split horizon, 235-236 IP forwarding EIGRPv4 (Enhanced Interior Gateway troubleshooting, 143-146 Routing Protocol version 4) ip address command, 134, 150, 160, advantages of, 232 185-186, 318 autosummarization, 270-272 IP addressing basic configuration, 253-254 binary-to-hexadecimal conversion, 566 compared to other routing protodecimal-to-binary conversion, 563-565 cols, 232-233, 238 hexadecimal-to-binary conversion, 566 convergence, 244-247, 265-266 IP ARP table, displaying, 588 development of, 231 ip domain-lookup command, 137 discontiguous classful networks, ip flow command, 497 271-272

DUAL (Diffusing Update Algorithm), 246	LSDB (link-state databases), 204-205
explained, 239	metrics, 224-225
feasible successors, 263-265	multi-area configuration, 217-220
hello packets, 237-238	neighbors, 202-206
load balancing, 267-269	RID (router ID), 202
loop avoidance, 244	self-assessment, 227
metric calculation, 269-270	single-area configuration, 218-219
metric components, 266-267	SPF route calculation, 208,
neighbors, 239-240	214-215
partial update messages, 237	verifying configuration, 220-223
route calculation, 241-245	OSPFv3 (Open Shortest Path First
self-assessment, 248-249, 274-275	version 3), 434
successors, 262-263	basic configuration, 435
topology table, viewing, 261-262	compared to OSPFv2, 441-442
update messages, 240-241	default routes, 440-441
variance, 268-269	interface cost, 439-440
verifying core features of, 255-260	interfaces, 443-444
wildcard masks, 255	<i>IPv6 routes</i> , 453-454
FHRP (First Hop Redundancy Protocol).	load balancing, 440
See FHRP	LSAs (link-state advertisements), 448-451
IP forwarding, troubleshooting, 143, 144-146	metrics, 451-453
normal routing behavior, predicting	multi-area configuration, 435-439
data link headers, 114-115	neighbors, 445-448
host IPv4 routing logic, 111-112	self-assessment, 456-457
IP routing from host to host,	single-area configuration, 436-438
113-114	problem isolation with ping command
IP routing logic on single router,	explained, 115-117
112-113	hostnames and IP addresses,
sample ARP process, 115	123-124
OSPFv2 (Open Shortest Path First	LAN neighbors, testing, 121-122
version 2), 200	longer routes, testing, 117-119
AD (administrative distance),	reverse routes, testing, 119-121
215-216	sample output, 116
areas, 206-213	WAN neighbors, testing, 122-123
basic configuration, 216-217	problem isolation with traceroute
compared to OSPFv3, 441-442	command, 124
compared to other routing proto-	explained, 124-126
cols, 232-233, 238	extended traceroute, 126-127
DRs (designated routers), 205-206	isolating problems to two routers,
explained, 201-202	127-129
fully neighbors, 206	sample output, 125
load balancing, 225	standard traceroute, 126
LSAs (link-state advertisements), 203-204, 209-213, 222	

protocol troubleshooting	ipv6 hold-time eigrp command, 4//
duplicate router IDs, 295-296	ipv6 ospf command, 432
EIGRP interfaces, 280-286	ipv6 ospf cost command, 440
EIGRP neighbors, 289-292	ipv6 ospf hello-interval command, 448
Hello/dead timer mismatches,	ipv6 router eigrp command, 463, 477
296-297	ipv6 router ospf command, 432
mismatched MTU settings, 299	IPv6 routing
mismatched network types, 297-299	EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6)
OSPF area mismatches, 294 OSPF interfaces, 280-281, 286-288	bandwidth and delay settings, 464-465
OSPF neighbors, 289-290, 293-297	basic configuration, 460-461
	compared to EIGRPv4, 466-467
overview, 279-280	configuration commands, 462
RIP-2, 232-233, 238	configuration example, 462-464
routing logic	explained, 461
from host to host, 113-114	interfaces, 467-469
on single router, 112-113	IPv6 routes, 472-473
routing table, displaying, 259-260	load balancing, 465
static routes, configuring, 582-585	neighbors, 469-470
troubleshooting, 110, 132-133	self-assessment, 475-476
ACLs (access control lists),	timers, 466
151-152, 585-588	topology database, 470-472
DHCP Relay issues, 140-141	host configuration
DNS problems, 136-137	router address, 415-416
IP address settings, 137	SLAAC (stateless address
IP forwarding, 143-146	autoconfiguration), 414-415
LAN issues, 141-142	stateful DHCPv6, 413-414
mismatched IPv4 settings, 133-134	static routes, 416-417
mismatched masks, 134-135	IOS packaging
mismatched VLAN trunking	explained, 527
configuration, 138-140	images per feature set combination, 528
normal routing behavior, predicting, 111-115	images per model/series, 527
with ping command, 115-124	universal images, 528
router WAN interface status,	IOS software activation, 529-530
150-151	Cisco License Manager (CLM),
with show ip route command,	530-531
144-146	manual activation, 531-536
with traceroute command, 124-129	right-to-use licenses, 536-538
VLSM, 146-150	self-assessment, 540
ipv6 address command, 415-416,	NetFlow
426-428, 432	collector, 500
ipv6 dhcp relay command, 425	configuring, 497-498
ipv6 dhcp relay destination command, 432	explained, 495-497
ipv6 eigrp asn command, 461	network flows, 497
ipv6 eigrp command, 463, 468, 477	verifying, 498-499
ipv6 hello-interval eigrp command, 477	

SNMP (Simple Network Management Protocol)	LAN neighbors, testing with ping, 121-122
community strings, 490	LAN switching
explained, 487-488	DPs (designated ports)
MIB (Management Information	choosing, 24-25
Base), 488-489	explained, 19
SNMP version 2c, 490-491	overview, 11
SNMP version 3, 491	root cost, 19
traps, 488	root switches
subnetting, 411-413	electing, 21-22
Syslog (System Message Logging)	explained, 19
configuring, 494-495	router LAN issues, troubleshooting,
explained, 492	141-142
Syslog server, 495	RPs (root ports)
system message format, 493	choosing, 23-24
system message severity levels, 494	explained, 19
verifying, 494-495	STP (Spanning Tree Protocol). See STP
troubleshooting	switch verification, 12
DNS issues, 424	determining VLAN of frames,
ping failures, 421-423	13-15
SLAAC issues, 425-426	switch reactions to changes with
stateful DHCP, 424-425	STP, 26-28
traceroute failures, 427-429	verifying trunks, 15
unicast IPv6 addresses, 411-413	viewing MAC address table, 12-13
verifying connectivity	troubleshooting, 64-65
from hosts, 417-418	analyzing/predicting normal
from routers, 419-420	operation, 65-68
ipv6 unicast-routing command, 415, 426, 432	ARP requests (broadcast), forwarding path of, 95-98
ISDN (Integrated Services Digital	cabling pinouts, 75
Network), 393-394	control plane analysis, 67-68
isolating	data plane analysis, 66-67
IPv4 routing problems	duplex issue, 77-78
ping command, 115-124	exam tips, 70
traceroute command, 124-129	example of, 91
LAN switching interface problems, 68-69, 73-78, 88-90	forwarding process overview,
cabling pinouts, 75	11-12, 71-72
interface status codes, 74-75	interface status codes, 74
notconnect state, 75	isolate filtering/port security problems, 79-82, 90-91
VLAN and trunking problems, 15, 82-86, 92-94	isolation of interface problems, 73-78, 88-90
V I	isolation of VLAN/trunking
K-L	problems, 15, 82-86, 92-94
keepalive command, 383	network diagram confirmation vid CDP, 72-73, 87-88
keepalive failure, troubleshooting, 327	notconnect state, 75

problem isolation, 68-69	leased lines, 387-388
R1 ARP Reply (unicast), forward-	license boot module command, 537, 541
ing path of, 98-101	license install command, 541
root cause analysis, 69-70	licensing (IOS), 526
switch interface speed and duplex,	IOS packaging
76-77	images per feature set
switch interface speeds, 77-78	combination, 528
layer 1 leased lines, 311-316	images per model/series, 527
building WAN links, 315-316	universal images, 528
CSU/DSU, 315	IOS software activation, 529-530
physical components, 312-314	Cisco License Manager (CLM),
T-carrier system, 314-315	530-531
troubleshooting, 325-326	manual activation, 531-536
layer 2 leased lines, 316-317, 326	right-to-use licenses, 536-538
layer 3 leased lines, 329-330	license status, showing, 533-534
LCP (Link Control Protocol), 321-323	permanent technology package license,
Learning state (STP), 28	adding, 535-536
leased line WANs (wide area networks)	self-assessment, 540
HDLC (High-level Data Link Control)	line status, 74
building WAN links, 315-316	Link Control Protocol (LCP), 321
CSU/DSU, 315	link-local addresses, 413
explained, 311	link-state advertisements. See LSAs
HDLC configuration, 317-320	link-state databases (LSDB), 204-205
layer 1 leased lines, 311-316	link-state routing protocols, OSPFv2,
layer 2 leased lines, 316-317	591-592
leased line components, 312-314	Link-State Update (LSU), 204, 234
T-carrier system, 314	link types, 576
PPP (Point-to-Point Protocol)	Listening state (STP), 28
authentication, 322-323	LMI (Local Management Interface),
CHAP (Challenge Handshake	337-341, 356
Authentication Protocol), 324-325, 328-329	load balancing
configuring, 323-324	EIGRPv4 (Enhanced Interior Gateway
explained, 320-321	Routing Protocol version 4), 267-269
framing, 321	EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 465
LCP (Link Control Protocol),	HSRP (Hot Standby Router Protocol),
321-322	162
NCP (Network Control Protocols),	OSPFv2 (Open Shortest Path First
321	version 2), 225
self-assessment, 332-333	OSPFv3 (Open Shortest Path First
troubleshooting	version 3), 440
keepalive failure, 327	PSVT+ (Per-VLAN Spanning Tree Plus),
layer 1 problems, 325-326	38
layer 2 problems, 326	local DLCI (data link connection
layer 3 problems, 329-330	identifiers), 342-343
PAP/CHAP authentication failure,	local loop, 393
328-329	

Local Management Interface (LMI),	math-related skills, 549-550		
337-341, 356	Max Age timers (STP), 26-28		
logging buffered command, 494	maximum-paths command, 225, 229,		
logging console command, 494	253, 267-269, 276, 440, 462, 465, 477		
logging with Syslog (System Message Logging)	memory (Flash), upgrading IOS software images into, 505-507		
configuring, 494-495	message logging. See Syslog		
explained, 492	metric calculation (EIGRP), 241-243		
Syslog server, 495	metrics		
system message format, 493 system message severity levels, 494	EIGRPv4 (Enhanced Interior Gateway Routing Protocol version 4), 266-270 OSPFv2 (Open Shortest Path First		
verifying, 494-495	version 2)		
Long-Term Evolution (LTE), 397	interface costs, 224		
loop avoidance, 244	reference bandwidth, 225		
LSAs (link-state advertisements)	MetroE (Metropolitan Ethernet), 389		
exchanging with neighbors, 203-204 explained, 209-210	MIB (Management Information Base),		
in multi-area design, 212-213	488-489		
network LSAs, 211-212	microseconds, 242		
OSPFv3 LSAs	mismatched IPv4 settings, 133-134 mismatched masks, 134-135		
troubleshooting, 450-451			
verifying, 448-450	mismatched MTU settings, 299		
router LSAs, 210	mismatched OSPF network types, 297-299		
verifying, 222	mismatched subnet numbers, 379		
LSDB (link-state databases), 204-205	mobile phone 3G/4G access, 397-398		
LSUs (Link-State Update), 204, 234 LTE (Long-Term Evolution), 397	MPLS (Multiprotocol Label Switching), 390-391		
M	mst parameter (spanning-tree mode command), 576		
	MTU settings, troubleshooting, 299		
MAC address table	multi-area design, LSAs (link-state		
STP (Spanning Tree Protocol), 17	advertisements) in, 212-213		
viewing, 12-13	multi-area OSPFv2 configuration,		
maintaining OSPFv2 neighbors, 204-205 Management Information Base (MIB), 488-489	217-223 multi-area OSPFv3 configuration, 435-439		
		manual software activation, 531-533	multiple frame transmission, 17
adding permanent technology package license, 535-536	multipoint subinterfaces, Frame Relay configuration, 366-368		
showing current license status, 533-534	Multiprotocol Interconnect over Frame		
mapping addresses (Frame Relay),	Relay, 342		
357-359	Multiprotocol Label Switching (MPLS),		
Inverse ARP, 360	390-391		
static mapping, 360-361			

troubleshooting, 377-378

N	network flows, 497
<u> </u>	network LSAs (link-state advertise-
name resolution (DNS), 123	ments), 211-212
NBMA (nonbroadcast multiaccess) net-	network management
works, 337-338	configuration files, 517-518
NDP (Neighbor Discovery Protocol), 413	copying, 519-520
neighbors	erasing, 519-520
EIGRPv4 neighbors, 239-240	running-config, 517
displaying status of, 258-259	setup mode, 521
troubleshooting, 289-292	startup-config, 517
verification checks, 290-291	IOS software
EIGRPv6 neighbors, 469-470	boot sequence, 507-513
OSPFv2 neighbors	upgrading images into Flash
adjacent neighbors, 206	memory, 505-507
area mismatches, 294	NetFlow
duplicate router IDs, 295-296	collector, 500
exchanging LSAs (link-state	configuring, 497-498
advertisement) with neighbors,	explained, 495-497
203-204	network flows, 497
Hello/dead timer mismatches,	verifying, 498-499
296-297	password recovery
forming neighbor relationships,	example, 515-517
202-203	explained, 513-515
fully adjacent neighbors, 206	self-assessment, 502-503
LSDB (link-state databases), 204-205	SNMP (Simple Network Management Protocol)
maintaining, 204-205	community strings, 490
states, 206	explained, 487-488
troubleshooting, 289-290, 293-297 OSPFv3 neighbors	MIB (Management Information Base), 488-489
troubleshooting, 446-448	SNMP version 2c, 490-491
verifying, 445-446	SNMP version 3, 491
NetFlow	traps, 488
collector, 500	Syslog (System Message Logging)
configuring, 497-498	configuring, 494-495
explained, 495-497	explained, 492
network flows, 497	Syslog server, 495
verifying, 498-499	system message format, 493
netsh interface ipv6 show neighbors	system message severity levels, 494
command, 433	verifying, 494-495
network area command, 217, 435	Network Management Station (NMS), 487
network command, 228, 253-255, 276, 280, 458, 461-462, 592	network types (OSPF), troubleshooting, 297-299
network diagrams, confirming via CDP (LAN switching), 72-73, 87-88	NMS (Network Management Station), 487
	no auto-summary command, 272, 276

no cdp enable command, 73	basic configuration, 216-217
no cdp run command, 73	compared to OSPFv3, 441-442
no frame-relay inverse-arp command, 383	compared to other routing protocols, 232-233, 238
no frame-relay lmi-type command, 372,	configuring, 592-595
383	default routes, 591-592
no ip domain-lookup command, 137	DRs (designated routers), 205-206
no ip split-horizon eigrp asn	explained, 201-202
command, 596	Frame Relay configuration, 368-369
no ipv6 eigrp 1 command, 469	load balancing, 225
no keepalive command, 365	LSAs (link-state advertisements)
no logging buffered command, 494	exchanging with neighbors,
no logging console command, 494	203-204
no passive-interface command, 229, 277	explained, 209-210
no shutdown command, 59, 80-81, 91,	in multi-area design, 212-213
318, 334, 477	network LSAs, 211-212
no shutdown vlan command, 84	router LSAs, 210
noAuthNoPriv security level, 492	verifying, 222
nonbroadcast multiaccess (NBMA)	LSDB (link-state databases), 204-205
networks, 337-338	metrics
notconnect state (LAN switches), 75	interface cost, 224
numeric reference table	reference bandwidth, 225
binary-to-hexadecimal conversion, 566	multi-area configuration, 217-220
decimal-to-binary conversion, 563-565	neighbors
hexadecimal-to-binary conversion, 566	
	adjacent neighbors, 206 area mismatches, 294
0	
	duplicate router IDs, 295-296
Open Shortest Path First. See OSPFv2; OSPFv3	exchanging LSAs with neighbors, 203-204
operating systems	forming neighbor relationships, 202-203
selection process, 509-511	Hello/dead timer mismatches,
three-router operating systems, 508-509	296-297
OSPF routes, 585	maintaining, 204-205
OSPFv2 (Open Shortest Path First	states, 206
version 2), 200	troubleshooting, 293-297
AD (administrative distance), 215-216	RID (router ID), 202
areas	self-assessment, 227
design advantages, 209	single-area configuration, 218-219
design rules, 207	SPF route calculation
design terminology, 207-208	calculating best routes, 214-215
explained, 206-207	reducing calculation time with
intra-area topology, 210-212	areas, 208
multi-area design, 212-213	troubleshooting
reducing SPF calculation time	area mismatches, 294
with, 208	
•	duplicate router IDs, 295-296

single-area OSPF, 206

Hello/dead timer mismatches, 296-297	P
interfaces, 280-281, 286-288 mismatched MTU settings, 299 mismatched network types, 297-299 neighbors, 289-297 network types, 297-299 overview, 279-280 verifying configuration, 220-223 areas, 221 DRs (dedicated routers) and BDRs (backup DRs), 221-222 LSAs (link-state advertisements), 222 OSPF routes, 223 OSPFv3 (Open Shortest Path First Version 3), 434 basic configuration, 435 compared to OSPFv2, 441-442 default routes, 440-441 interfaces, 443 cost, 439-440 troubleshooting, 443-444 verifying, 443 IPv6 routes, troubleshooting, 453-454 load balancing, 440 LSAs (link-state advertisements) troubleshooting, 450-451 verifying, 448-450 metrics, verifying, 451-453 multi-area configuration, 435-439 neighbors troubleshooting, 446-448 verifying, 445-446 self-assessment, 456-457 single-area configuration, 436-438 overlapping subnets configuring, 149-150 with VLSM, 148-149 without VLSM, 147-148	packaging (IOS) explained, 527 images per feature set combination, 528 images per model/series, 527 universal images, 528 packet filtering with ACLs (access control lists), 151-152 PAP/CHAP authentication failure, 328-329 partial-mesh networks, 340 partial update messages, 237 passive-interface command, 229, 257, 277, 280-281, 285, 301, 444 passive-interface default command, 229, 277 password recovery example, 515-517 explained, 513-515 periodic update messages, 234 permanent keyword (ip route command) 583-584 permanent virtual circuits (PVC), 338, 372-377 Per-VLAN Spanning Tree Plus (PVST+), 38 physical subinterfaces, EIGRP on, 595-597 PID (product ID), 531 ping command, 418-419, 432-433 extended ping  LAN neighbors, testing, 122 reverse routes, testing, 119-121 IPv4 testing explained, 115-117 with bostnames and IP addresses, 123-124 LAN neighbors, 121-122 longer routes, 117-119 reverse routes, 119-121 sample output, 116
without VLSM, 147-148	

troubleshooting in IPv4	PoP (point of presence), 393
neighboring devices over	port roles, configuring, 579-580
Ethernet, 588	port states, 574-575, 580
over serial links with ACLs (access	port types, 576, 581
control lists), 585-588	PortFast, 30, 46-47
troubleshooting in IPv6, 421-423	ports
ping6 command, 418, 433	alternate (root) ports, 573-574
pinouts (cabling) for LAN switches, 75	DPs (designated ports)
point of presence (PoP), 393	choosing, 24-25
point-to-multipoint subinterfaces, EIGRP	determining, 54-55
on, 595-597	explained, 19
point-to-point edge ports, 576	RSTP (Rapid Spanning Tree
point-to-point links, 576	Protocol), 575-576
point-to-point ports, 576	strategies for DP exam questions,
Point-to-Point Protocol. See PPP	55-56
point-to-point subinterfaces	point-to-point edge ports, 576
configuring, 361-364	point-to-point ports, 576
EIGRP on, 595-597	port costs, 25-26
point-to-point WANs (wide area networks)	port states, 574,575,580
HDLC (High-level Data Link Control)	port states, 574-575, 580
building WAN links, 315-316	RPs (root ports)  choosing, 23-24
CSU/DSU, 315	8
	determining, 52
explained, 311 HDLC configuration, 317-320	explained, 19
layer 1 leased lines, 311-316	RSTP (Rapid Spanning Tree Protocol), 573-574
	STP tiebreakers when choosing RP,
layer 2 leased lines, 316-317	53-54
leased line components, 312-314	strategies for RP exam questions, 54
<i>T-carrier system</i> , 314 PPP (Point-to-Point Protocol)	security
authentication, 322-323	configuring on Cisco Catalyst
CHAP (Challenge Handshake	switches, 80
Authentication Protocol),	LAN switching, 79-82, 90-91
324-329	shared ports, 576
configuring, 323-324	STP (Spanning Tree Protocol) port cost,
explained, 320-321	43-45
framing, 321	powers of 2 numeric reference table, 567
LCP (Link Control Protocol),	ppp authentication command, 334
321-322	PPP (Point-to-Point Protocol)
NCP (Network Control Protocols),	LCP authentication, 323
321	leased-line WANs
troubleshooting	authentication, 322-323
keepalive failure, 327	CHAP (Challenge Handshake
layer 1 problems, 325-326	Authentication Protocol),
layer 2 problems, 326	324-329
layer 3 problems, 329-330	configuring, 323-324
PAP/CHAP authentication failure, 328-329	explained, 320-321

PVC (permanent virtual circuits) framing, 321 LCP (Link Control Protocol), Frame Relay, 338 321-322 status codes, 376 NCP (Network Control Protocols), subinterface status, 377 321 troubleshooting in Frame Relay, 372-377 PPPoE (PPP over Ethernet) pvst parameter (spanning-tree mode configuring, 399-400 command), 577 explained, 398-399 PVST+ (Per-VLAN Spanning Tree Plus), 38 pppoe-client command, 400 practice exams, 551-553 exam-taking tips, 553-554 Question Review, 554-556 query/reply process (EIGRP), 246-247 predicting normal IPv4 routing behavior Question Review, 554-556 data link headers, 114-115 question types (Cisco Certification Exam), 546-547 host IPv4 routing logic, 111-112 IP routing from host to host, 113-114 R IP routing logic on single router, 112-113 sample ARP process, 115 pre-exam suggestions (Cisco Rapid Spanning Tree Protocol. See RSTP Certification Exam), 548 (Rapid Spanning Tree Protocol) rapid-pvst parameter (spanning-tree PRI (Primary Rate Interface), 394 mode command), 579 Primary Rate Interface (PRI), 394 RD (reported distance), 244-245 priority of switches, configuring, 45-46 read-only (RO) community strings, 490 private WANs (wide area networks) read-write (RW) community strings, 490 explained, 387 recovering Frame Relay, 388 passwords leased lines, 387-388 example, 515-517 problem isolation *explained*, 513-515 IPv4 routing problems recovery if IOS does not load, 511 ping command, 115-124 redundancy. See FHRP (First Hop traceroute command, 124-129 Redundancy Protocol) LAN switching, 68-69 reference bandwidth, 224-225 product ID (PID), 531 Relay (DHCP), troubleshooting, 140-141 protocol status, 74 releases, 527 protocols. See specific protocols Reliable Transport Protocol (RTP), 240 psvt parameter (spanning-tree mode reload command, 519, 525 command), 576 remote-access VPNs (virtual private public WANs (wide area networks) networks), 178 3G/4G mobile phone access, 397-398 replies (ARP), forwarding path of, 98-101 Cable Internet, 396 reported distance (RD), 244-245 dial access with modems and ISDN, requests 393-394 ARP requests (broadcast), forwarding path of, 95-98 DSL (digital subscriber line), 395-396 ICMP Echo Requests, 127 Internet Access Links, 392 resetting passwords PPPoE (PPP over Ethernet) example, 515-517 configuring, 399-400 explained, 514-515 explained, 398-399

reverse routes, 127	routing table (IPv4), displaying, 259-260
RID (router ID), 202	RPs (root ports)
right-to-use licenses, 536-538	choosing, 23-24
RIP steady-state operations, 234-235	determining, 52
RIP-2, 232-233, 238	explained, 19
RO (read-only) community strings, 490	RSTP (Rapid Spanning Tree Protocol),
ROAS (Router on a Stick), 138-140	573-574
ROMMON mode, 508, 514-515	STP tiebreakers when choosing RP, 53-54
root cause analysis, 69-70	strategies for RP exam questions, 54
root cost, 19	RSTP (Rapid Spanning Tree Protocol),
root ports (RPs)	29-31, 572-573
choosing, 23-24	alternate (root) ports, 573-574
determining, 52	backup (designated) ports, 575-576
explained, 19	capabilities, 571-572
RSTP (Rapid Spanning Tree Protocol),	configuring
573-574	identifying STP mode on Catalyst
STP tiebreakers when choosing RP, 53-54	switches, 577-579
strategies for RP exam questions, 54	port roles, 579-580
root switches	port states, 574-575, 580
determining, 51-52	port types, 576, 581
electing via STP, 21-22	link types, 575
route calculation (EIGRPv4)	point-to-point ports, 576
bandwidth issues, 243	shared ports, 576
example, 242-243	RTP (Reliable Transport Protocol), 240
FD (feasible distance), 244-245	running-config, 517
metric calculation, 241	RW (read-write) community strings, 490
RD (reported distance), 244-245	RxBoot operating system, 508
route poisoning, 236-237	
route redistribution, 215	S
router eigrp command, 253-254, 276,	
286, 462	scalability
router ID (RID), 202	OSPFv2 with areas
router-id command, 202, 216, 229,	design advantages, 209
435-437, 458	design rules, 207
router LSAs (link-state advertisements),	design terminology, 207-208
210	explained, 206-207
Router on a Stick (ROAS), 138-140	intra-area topology, 210-212
router ospf command, 216, 228, 286,	multi-area design, 212-213
435, 458	reducing SPF calculation time
routers	with, 208
active virtual gateway (AVG), 163	single-area OSPF, 206
address configuration, 415-416	VPNs (virtual private networks), 179
clock speed, 316-317	Secure Shell (SSH), 115
FHRP (First Hop Redundancy Protocol).  See FHRP	Secure Socket Layer (SSL) VPNs, 181
for VPNs (virtual private networks), 179	security
routing. See IPv4 routing; IPv6 routing	port security, 79-82, 90-91
Touring, see if v4 fouring; if vo fouring	VPNs (virtual private networks), 177

routing protocols, OSPFv2, 591-592

securityk9, 530	show cdp neighbors detail command, 73
self-assessments	show command, 92, 463, 577
EIGRPv4 (Enhanced Interior Gateway	show controllers command, 319
Routing Protocol version 4), 248-249, 274-275	show controllers serial command, 318, 335
EIGRPv6 (Enhanced Interior Gateway	show etherchannel command, 48, 63
Routing Protocol version 6), 475-476	show etherchannel summary command, 58
FHRP (First Hop Redundancy Protocol), 170-172	show flash command, 507, 525
Frame Relay, 349-350, 381-382	show frame-relay lmi command, 371-372, 383
IOS file management, 505, 523-524 IOS licensing, 540	show frame-relay map command, 359-360, 365, 368, 375, 378, 384
leased-line WANs, 332-333 network management, 502-503	show frame-relay pvc command, 359, 365, 374-376, 383
OSPFv2 (Open Shortest Path First	show glbp brief command, 167-168
version 2), 227	show glbp command, 169
OSPFv3 (Open Shortest Path First version 3), 456-457	show interface switchport command, 83-85
STP (Spanning Tree Protocol), 32-34, 60-61	show interfaces command, 74-78, 89, 224, 241, 269, 301, 324, 334, 379,
VPNs (virtual private networks), 190-191	383-384
WAN (wide area network) technologies, 402	show interfaces description command, 74, 142-143, 301, 320
self ping, 586-587 serial cables, 313	show interfaces status command, 13-15, 74-77, 88
serial links, troubleshooting, 325	show interfaces trunk command, 15, 84
ACLs (access control lists), 585-588	show interfaces tunnel command, 187
keepalive failure, 327	show ip access-lists command, 152
layer 1 problems, 325-326	show ip cache flow command, 499
layer 2 problems, 326	show ip eigrp interface command, 257, 287
layer 3 problems, 329-330	show ip eigrp interfaces command, 256,
PAP/CHAP authentication failure, 328-329	277, 280-286, 301
serial number (SN), 531	show ip eigrp interfaces detail command, 256, 277
servers, Syslog, 495 service providers, 312	show ip eigrp neighbors command, 258, 277, 290, 301
session keys, 180	show ip eigrp topology all-links
setup command, 521, 525	command, 265
setup mode, 521	show ip eigrp topology command,
severity levels (Syslog), 494	241, 261-266, 277
shared keys, 180 shared ports, 576	show ip flow export command, 499
shared session keys, 180	show ip flow interface command, 499
show access-lists command, 152	show ip interface brief command, 187,
show arp command, 137	288, 320, 334, 379, 384
show cdp command, 73	show ip interface command, 151
show cdp command, 73 show cdp entry command, 73, 87	show ip interfaces command, 151-152
show cdp entry command, 73, 87 show cdp neighbors command, 73, 87	show ip ospf command, 229, 301, 458
show cup heighbors command, 73, 67	show ip sopf interface command, 594

show ip opsf interface brief command, 287 show ip ospf database command, 209, 222, 229, 459 show ip ospf interface brief command, 221, 229, 281, 286, 301, 458 show ip ospf interface command, 221-222, 229, 296, 301, 459 show ip ospf neighbor command, 202-203, 206, 222, 229, 293, 301, 459 show ip protocols command, 221, 229, 256-259, 277, 280, 282-288, 291, 301, 459, 593 show ip route command, 144-145, 188, 216, 229, 260, 271, 277, 459, 465, 583, 585 command output, 145-146 finding best route with, 145 overlapping routes, 144 show ip route eigrp command, 259-260, 284, 301 show ip route ospf command, 144, 229, 301, 459 show ip route | section command, 277 show ip route static command, 583 ship ip route subnet command, 585 show ipv6 eigrp interfaces command, 467-468, 477 show ipv6 eigrp interfaces detail command, 478 show ipv6 eigrp neighbors command, 469-470, 478 show ipv6 eigrp topology command, 471, 478 show ipv6 eigrp topology | section command, 478 show ipv6 interface command, 429, 432 show ipv6 neighbors command, 420, 432 show ipv6 ospf command, 432, 453 show ipv6 ospf database command, 432 show ipv6 ospf interface brief command, 432, 443-444, 453 show ipv6 ospf interface command, 443-444, 448 show ipv6 ospf neighbor command, 432, 445-447, 451 show ipv6 protocols command, 432, 443, 468-470, 478 show ipv6 route command, 432, 465, 478

show ipv6 route eigrp command, 478 show ipv6 route ospf command, 452 show ipv6 route | section command, 478 show ipv6 routers command, 432 show license command, 534, 537 show license feature command, 534, 541 show license udi command, 531-532, 541 show logging command, 494-495 show mac address-table command, 13, 83, 100 show mac address-table dynamic command, 12, 83, 100 show port-security command, 90 show port-security interface command, 79-81 show running-config command, 47, 152, 256, 318, 443, 518, 525 show spanning-tree bridge command, show spanning-tree command, 42, 49-56, 63, 581 show spanning-tree interface command, 63 show spanning-tree root command, 42, 46, 51-52, 63 show spanning-tree vlan command, 41-42, 51, 63, 84, 95, 579-580 show standby brief command, 165-166 show standby command, 166-167 show startup-config command, 518 show version command, 512-513, 534-536, 541 show vlan brief command, 14, 83 show vlan command, 14, 83 show vlan id command, 83 shutdown command, 59, 81, 91, 334, 477 Simple Network Management Protocol. See SNMP single-area OSPF (Open Shortest Path First), 206 single-area OSPFv2 configuration, 218-219 single-area OSPFv3 configuration, 436-438 single points of failure, 157-158 site-to-site VPNs (virtual private networks), 177-178 SLAAC (stateless address autoconfigura-

tion), 411, 414-415, 425-426

SMARTnet, 529	spanning-tree vlan vlan-id priority value
SN (serial number), 531	command, 45
SNMP (Simple Network Management Protocol)	spanning-tree vlan vlan_id priority x command, 39, 62
community strings, 490	spanning-tree vlan vlan-id root primary
explained, 487-488	command, 45
MIB (Management Information Base), 488-489	spanning-tree vlan vlan-id root secondary command, 45
SNMP version 2c, 490-491 SNMP version 3, 491	spanning-tree vlan vlan-number port- priority priority command, 62
traps, 488	spanning-tree vlan vlan-number root secondary command, 62
snmp-server community command, 490	
snmp-server contact command, 490	spanning-tree vlan x cost command, 40, 43-44, 62
snmp-server location command, 490	speed command, 77
SNMPGET utility, 489	SPF route calculation
software activation (IOS), 529-530	calculating best routes, 214-215
Cisco License Manager (CLM), 530-531	reducing calculation time with areas, 208
manual activation	split horizon, 235-236, 595-597
activation process, 531-534	SSH (Secure Shell), 115
adding permanent technology	SSL (Secure Socket Layer) VPNs, 181
package license, 535-536	STA (spanning tree algorithm), 19
right-to-use licenses, 536-538	standby command, 164
self-assessment, 540	startup-config, 517
spanning tree algorithm (STA), 19	stateful DHCPv6, 413-414, 424-425
Spanning Tree Protocol. See STP	stateless address autoconfiguration
spanning-tree bpduguard default command, 47	(SLAAC), 411, 414-415, 425-426
spanning-tree bpduguard disable	states of OSPFv2 neighbors, 206
command, 47, 63	states (port), 574-575, 580
spanning-tree bpduguard enable	static address mapping, 360-361
command, 46-47, 63	static router configuration (IPv6), 416-417
spanning-tree cost command, 56	static routes, configuring, 582-583
spanning-tree mode command, 62, 577,	with competing routes, 584-585
580	with no competing routes, 583
spanning-tree mode mst command, 38	steady-state networks (STP), 26
spanning-tree mode pvst command, 38, 577	steady-state operations (RIP), 234-235 STP (Spanning Tree Protocol), 10, 36
spanning-tree mode rapid-pvst command, 38, 579	BID (bridge ID), 20 blocking state, 18-20
spanning-tree portfast bpduguard default command, 63	BPDU (bridge protocol data units), 20-21 BPDU Guard feature, 30-31
spanning-tree portfast command, 46-47,	broadcast storms, 16-17
63	configuring
spanning-tree portfast default command, 47, 63	BID (bridge ID), 39-40
spanning-tree portfast disable command,	BPDU Guard, 46-47
47, 63	defaults and configuration options,
,	40

EtherChannel, 47-50	self-assessment, 32-34, 60-61
per-VLAN configuration settings,	STA (spanning tree algorithm), 19
38-39	state comparison table, 28
per-VLAN costs, 40	steady-state networks, 26
port costs, 44	timers, 26-28
PortFast, 46-47	topology
STP mode, 37-38	influencing with configuration
STP port costs, 43-45	changes, 25-26
switch priority, 44-46	interface state changes, 28-29
system ID extension, 39-40	reacting to state changes that affec
convergence, 19, 28	STP topology, 26
delays, 28	simple STP tree, 18-19
troubleshooting, 56	switch reactions to changes with
DPs (designated ports)	STP, 26-28
choosing, 24-25	troubleshooting, 51
determining, 54-55	convergence, 56
explained, 19	DPs (designated ports), 54-56
strategies for DP exam questions,	EtherChannel, 56-59
55-56	root switches, 51-52
EtherChannel, 29-30	RPs (root ports), 52-54
explained, 15-16	verifying default operation, 42
forwarding state, 18-19	verifying STP operation, 40-43
reasons for, 20	subinterfaces, 346
root switches, 19-22	multipoint subinterfaces, 366-368
interface state changes, 28-29	point-to-point subinterfaces, configuring
Learning state, 28	361-364
Listening state, 28	subnet masks, troubleshooting, 134-135
MAC table instability, 17	subnets, 549-550
multiple frame transmission, 17	Frame Relay networks
need for, 16-17	fully meshed networks with one II
port costs, 25-26	subnet, 354-355
PortFast, 30	hybrid Layer 3 addressing,
PSVT+ (Per-VLAN Spanning Tree Plus),	347-348
38	one subnet containing all Frame Relay DTEs, 345
root switches	one subnet per VC, 345-346
determining, 51-52	IPv6, 411-413
electing, 21-22	mismatched masks, troubleshooting,
RPs (root ports)	134-135
choosing, 23-24	mismatched subnet numbers, trouble-
determining, 52	shooting, 379
explained, 19	overlapping subnets
STP tiebreakers when choosing RP,	configuring, 149-150
53-54	with VLSM, 148-149
strategies for RP exam questions, 54	without VLSM, 147-148
RSTP (Rapid Spanning Tree Protocol).  See RSTP	

successors (EIGRP), 245-246	longer routes, 117-119
feasible successors, 265	reverse routes, 119-121
finding, 262-263	WAN neighbors, 122-123
superior hello (STP), 21	time burners, 547
SVC (switched virtual circuits), 338	time-division multiplexing (TDM), 314
switch priority, configuring, 45-46	time management (Cisco Certification
switch verification (LAN)	Exam), 547-548
determining VLAN of frames, 13-15	Time To Live (TTL), 125
verifying trunks, 15	Time-to-Live Exceeded (TTL Exceeded),
viewing MAC address table, 12-13	125
switchport access vlan command,	timers
83, 92, 140	Dead Interval, 204
switchport mode access command, 82, 140	EIGRPv6, 466
switchport mode trunk command, 82, 139	Hello/dead timer mismatches, 296-297
switchport port-security command, 82	Hello Interval, 204
switchport port-security mac-address	topology table
command, 82, 100	EIGRPv4
switchport port-security mac-address	convergence, 265-266
sticky command, 82	feasible successor routes, 263-265
switchport port-security violation	successor routes, 262-263
command, 79, 82	viewing, 261-262
switchport trunk allowed vlan command, 84	EIGRPv6, 470-472
switchport trunk mode command, 85	traceroute command, 124, 418-419,
switchport trunk mode command, os	432-433
139	explained, 124-126
Syslog (System Message Logging)	extended traceroute, 126-127
configuring, 494-495	GRE (generic routing encapsulation) tunnels, verifying, 188
explained, 492	isolating problems to two routers,
Syslog server, 495	127-129
system message format, 493	sample output, 125
system message severity levels, 494	standard traceroute, 126
verifying, 494-495	troubleshooting in IPv6, 427-429
system ID extension, configuring, 39-40	traceroute6 command, 433
System Message Logging. See Syslog	traps (SNMP), 488
	Triple DES (3DES), 180
T	troubleshooting
	CHAP (Challenge Handshake
T-carrier system, 314	Authentication Protocol), 328-329
tables, MAC address tables, 12-13, 17	EIGRPv4 (Enhanced Interior Gateway
TDM (time-division multiplexing), 314	Routing Protocol version 4)
tens-of-microseconds, 242	interfaces, 280-286
testing IPv4 routing with ping command	neighbors, 289-292
with hostnames and IP addresses, 123-124	overview, 279-280
LAN neighbors, 121-122	

EtherChannel, 56	ARP requests (broadcast),
channel-group command options,	forwarding path of, 95-98
57-58	cabling pinouts, 75
interface configuration settings,	control plane analysis, 67-68
58-59	data plane analysis, 66-67
Frame Relay, 369	duplex issues, 77-78
end-to-end encapsulation, 378	exam tips, 70
Layer 1 issues on access links, 370	example of, 91
Layer 2 issues on access links, 371	forwarding process overview,
mapping issues, 377-378	11-12, 71-72
mismatched subnet numbers, 379	interface status codes, 74
PVC (permanent virtual circuit) problems, 372-377	isolate filtering/port security problems, 79-82, 90-91
self-assessment, 381-382	isolation of interface problems,
suggested process, 369-370	73-78, 88-90
IPv4 routing, 110, 132-133	isolation of VLAN/trunking
ACLs (access control lists), 151-152, 585-588	problems, 15, 82-86, 92-94 network diagram confirmation via
DHCP Relay issues, 140-141	CDP, 72-73, 87-88
DNS problems, 136-137	notconnect state, 75
•	problem isolation, 68-69
IP address settings, 137	root cause analysis, 69-70
IP forwarding, 143-146 LAN issues, 141-142	switch interface speed and duplex,
•	76-77
mismatched IPv4 settings, 133-134 mismatched masks, 134-135	switch interface speeds, 77-78
•	OSPFv2 (Open Shortest Path First
mismatched VLAN trunking configuration, 138-140	version 2)
normal routing behavior,	area mismatches, 294
predicting, 111-115	duplicate router IDs, 295-296
with ping command, 115-124	Hello/dead timer mismatches, 296-297
router WAN interface status,	interfaces, 280-281, 286-288
150-151	mismatched MTU settings, 299
with show ip route command, 144-146	mismatched network types,
with traceroute command, 124-129	297-299
VLSM, 146-150	neighbors, 289-297
IPv6 routing, 421	overview, 279-280
DNS issues, 424	OSPFv3 (Open Shortest Path First version 3)
ping failures, 421-423	interfaces, 443-444
SLAAC issues, 425-426	IPv6 routes, 453-454
stateful DHCP, 424-425	LSAs (link-state advertisements),
traceroute failures, 427-429	450-451
LAN switching, 64-65	neighbors, 446-448
analyzing/predicting normal operation, 65-68	serial links
ARP Reply (unicast), forwarding	keepalive failure, 327
path of, 98-101	layer 1 problems, 325-326

layer 2 problems, 326 layer 3 problems, 329-330 PAP/CHAP authentication failure, 328-329 STP (Spanning Tree Protocol), 51 convergence, 56 DPs (designated ports), 54-56 EtherChannel, 56-59	unicast IPv6 addresses, 411-413 unicasts, forwarding, 99-100 unique device identifier (UDI), 531 universal images explained, 528 IOS software activation, 529-530 Cisco License Manager (CLM), 530-531
root switches, 51-52	manual activation, 531-536
<i>RPs (root ports), 52-54</i> VLSM, 146	right-to-use licenses, 536-538 unsecured networks, GRE (generic rout-
	ing encapsulation) tunnels, 183-184
overlapping subnets, 148-150 recognizing when VLSM is used,	update messages (EIGRP), 240-241
147	upgrading images into Flash memory,
trunking	505-507
mismatched VLAN trunking configuration, 138-140	username command, 334
trunking problems, isolating, 15, 82-86, 92-94	V
verifying, 15, 93-94	variance, 268-269
TTL (Time To Live), 125	variance, 200-207 variance command, 253, 268-269, 276,
TTL (Time-to-Live) Exceeded, 125	462, 465, 477
tunnel destination command, 186, 192	VC (virtual circuits)
tunnel interfaces, 182-184	CIR (committed information rate), 338
tunnel mode gre command, 192	explained, 337-340, 345-346
tunnel source command, 186, 192	verifying
tunnels	EIGRPv4 core features, 255
explained, 178	interfaces, 256-258
GRE (generic routing encapsulation)	<i>IPv4 routing table, 259-260</i>
tunnels	neighbor status, 258-259
configuring, 185-187	neighbors, 290-291
explained, 181-182	Frame Relay configurations, 364-365
over unsecured network, 183-184	GLBP (Gateway Load Balancing
routing over, 182-183	Protocol), 167-169
tunnel interfaces, 182-184	GRE (generic routing encapsulation)
verifying, 187-189	tunnels, 187-189
VPN tunnels, 177-178	HSRP (Hot Standby Router Protocol),
Two-way neighbor state (OSPF	164-167
neighbors), 206	IOS images, 512-513
	IPv6 connectivity
U	from hosts, 417-418
	from routers, 419-420
uck9, 530	LAN switches
UDI (unique device identifier), 531 undebug all command, 302	determining VLAN of frames, 13-15
unequal-cost load balancing, 268	verifying trunks, 15

viewing MAC address table, 12-13

NetFlow, 498-499	trunking
OSPFv2 (Open Shortest Path First	mismatched VLAN trunking con-
version 2), 220-223	figuration, 138-140
areas, 221	verifying, 93-94
configuration, 593-594	VLSM, troubleshooting, 146
DRs (dedicated routers) and BDRs	overlapping subnets, 148-150
(backup DRs), 221-222	recognizing when VLSM is used, 147
LSAs (link-state advertisements),	VPLS (Virtual Private LAN Service), 389
222	•
OSPF routes, 223	VPNs (virtual private networks)
OSPFv3 (Open Shortest Path First ver-	ASA (Adaptive Security Appliances), 179
sion 3)	=- /
interfaces, 443	clients, 179
LSAs (link-state advertisements),	explained, 176
448-450	extranet VPNs, 178
metrics, 451-453	GRE (generic routing encapsulation)
neighbors, 445-446	tunnels
STP (Spanning Tree Protocol) operation,	configuring, 185-187
40-43	explained, 181-182
Syslog (System Message Logging),	over unsecured network, 183-184
494-495	routing over, 182-183
trunking and VLAN 3, 93-94	tunnel interfaces, 182-184
ery small aperture terminal (VSAT), 391	verifying, 187-189
rirtual circuits (VC)	intranet VPNs, 178
explained, 337-340	IPsec VPNs, 179-180
Layer 3 addressing, 345-346	remote-access VPNs, 178
Virtual Private LAN Service (VPLS), 389	routers, 179
rirtual private networks. See VPNs	scalability, 179
Firtual Router Redundancy Protocol	security, 177
(VRRP), 160	self-assessment, 190-191
/LANs	site-to-site VPNs, 177
access interface VLAN assignments,	SSL VPNs, 181
checking, 92	tunnels, 177
active VLANs, checking for, 92-93	VPN tunnels, 177-178
broadcast forwarding, 97-98	VRRP (Virtual Router Redundancy
determining VLAN of frames, 13-15	Protocol), 160, 590
isolating VLAN and trunking problems,	VSAT (very small aperture terminal), 391
15, 82-86, 92-94	
STP (Spanning Tree Protocol)	W-X-Y-Z
configuration	
BID (bridge ID), 39-40	WAN interface cards (WICs), 313
per-VLAN configuration settings,	WANs (wide area networks)
38-39	Frame Relay. See Frame Relay
per-VLAN costs, 40	HDLC (High-level Data Link Control)
system ID extension, 39-40	building WAN links, 315-316
	CSII/DSII 315

explained, 311

HDLC configuration, 317-320	PAP/CHAP authentication failure,
layer 1 leased lines, 311-316	328-329
layer 2 leased lines, 316-317	VPNs (virtual private networks)
leased line components, 312-314	ASA (Adaptive Security
self-assessment, 332-333	Appliances), 179
T-carrier system, 314	clients, 179
neighbors, testing with ping, 122-123	explained, 176
PPP (Point-to-Point Protocol)	extranet VPNs, 178
authentication, 322-323	GRE (generic routing encapsula-
CHAP (Challenge Handshake	tion) tunnels, 181-189
Authentication Protocol),	intranet VPNs, 178
324-329	IPsec VPNs, 179-180
configuring, 323-324	remote-access VPNs, 178
explained, 320-321	routers, 179
framing, 321	scalability, 179
LCP (Link Control Protocol),	security, 177
321-323	self-assessment, 190-191
NCP (Network Control Protocols),	site-to-site VPNs, 177
321	SSL VPNs, 181
private WANs	tunnels, 177
Ethernet WANs, 389-390	VPN tunnels, 177-178
explained, 387	WICs (WAN interface cards), 313
Frame Relay, 388	wildcard masks, configuring EIGRPv4
leased lines, 387-388	with, 255
MPLS (Multiprotocol Label Switching), 390-391	wireless Internet, 397
VSAT (very small aperture termi-	write erase command, 520, 525
nal), 391	
public WANs, 392	
3G/4G mobile phone access,	
397-398	
Cable Internet, 396	
dial access with modems and	
ISDN, 393-394	
DSL (digital subscriber line),	
395-396	
Internet Access Links, 392	
PPPoE (PPP over Ethernet), 398-400	
router WAN interface status, troubleshooting, 150-151	
self-assessment, 402	
troubleshooting	
keepalive failure, 327	
layer 1 problems, 325-326	
layer 2 problems, 326	
layer 3 problems, 329-330	