CISCO

Official Cert Guide

Learn, prepare, and practice for exam success

INCLUDES
CCNA Simulator Lite Software
60 Minutes of Video Training
More than **350 Practice Exam Questions**

Cisco CCNA

Routing and Switching ICND2 200-101

ciscopress.com

WENDELL ODOM, CCIE® No. 1624

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 troubleshooting 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 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

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

Wendell Odom, CCIE No. 1624

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

Printed in the United States of America

Ninth Printing: April 2015

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58714-373-1

ISBN-10: 1-58714-373-9

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.

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 troubleshoot 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*) 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 xxviii

Getting Started 3

Part I: LAN Switching 11

Chapter 1: Spanning Tree Protocol Concepts 13

Chapter 2: Spanning Tree Protocol Implementation 43

Chapter 3: Troubleshooting LAN Switching 77

Part I Review 124

Part II: IP Version 4 Routing 129

Chapter 4: Troubleshooting IPv4 Routing Part I 131

Chapter 5: Troubleshooting IPv4 Routing Part II 157

Chapter 6: Creating Redundant First-Hop Routers 183

Chapter 7: Virtual Private Networks 205

Part II Review 224

Part III: IP Version 4 Routing Protocols 229

Chapter 8: Implementing OSPF for IPv4 231

Chapter 9: Understanding EIGRP Concepts 267

Chapter 10: Implementing EIGRP for IPv4 291

Chapter 11: Troubleshooting IPv4 Routing Protocols 323

Part III Review 352

Part IV: Wide Area Networks 357

Chapter 12: Implementing Point-to-Point WANs 359

Chapter 13: Understanding Frame Relay Concepts 389

Chapter 14: Implementing Frame Relay 409

Chapter 15: Identifying Other Types of WANs 445

Part IV Review 464

Part V: IP Version 6 469

Chapter 16: Troubleshooting IPv6 Routing 471

Chapter 17: Implementing OSPF for IPv6 499

Chapter 18: Implementing EIGRP for IPv6 529

Part V Review 550

Part VI: Network Management 555

Chapter 19: Managing Network Devices 557

Chapter 20: Managing IOS Files 579

Chapter 21: Managing IOS Licensing 605

Part VI Review 624

Part VII: Final Review 627

Chapter 22: Final Review 629

Part VIII: Appendixes 647

Appendix A: Numeric Reference Tables 649

Appendix B: ICND2 Exam Updates 657

Glossary 687

Index 706

DVD Appendixes

Appendix C Answers to the "Do I Know This Already?" Quizzes

Appendix D Memory Tables

Appendix E Memory Tables Answer Key

Appendix F Mind Map Solutions

Appendix G Study Planner

Contents

Introduction xxviii

Getting Started 3

Part I: LAN Switching 11

Chapter 1 Spanning Tree Protocol Concepts 13

"Do I Know This Already?" Quiz 13

Foundation Topics 16

LAN Switching Review 16

LAN Switch Forwarding Logic 16

Switch Verification 17

Viewing the MAC Address Table 17

Determining the VLAN of a Frame 19

Verifying Trunks 20

Spanning Tree Protocol (IEEE 802.1D) 21

The Need for Spanning Tree 22

What IEEE 802.1D Spanning Tree Does 24

How Spanning Tree Works 25

The STP Bridge ID and Hello BPDU 27

Electing the Root Switch 27

Choosing Each Switch's Root Port 29

Choosing the Designated Port on Each LAN Segment 31

Influencing and Changing the STP Topology 32

Making Configuration Changes to Influence the STP Topology 32

Reacting to State Changes That Affect the STP Topology 33

How Switches React to Changes with STP 34

Changing Interface States with STP 35

Optional STP Features 36

EtherChannel 37

PortFast 37

BPDU Guard 38

Rapid STP (IEEE 802.1w) 38

Exam Preparation Tasks 40

Chapter 2 Spanning Tree Protocol Implementation 43

"Do I Know This Already?" Quiz 43

Foundation Topics 46

STP Configuration and Verification 46
Setting the STP Mode 47
Connecting STP Concepts to STP Configuration Options 47
Per-VLAN Configuration Settings 47
The Bridge ID and System ID Extension 48
Per-VLAN Port Costs 49
STP Configuration Option Summary 49
Verifying STP Operation 50
Configuring STP Port Costs 53
Configuring Priority to Influence the Root Election 55
Configuring PortFast and BPDU Guard 56
Configuring EtherChannel 58
Configuring a Manual EtherChannel 58
Configuring Dynamic EtherChannels 60
STP Troubleshooting 61
Determining the Root Switch 62
Determining the Root Port on Nonroot Switches 63
STP Tiebreakers When Choosing the Root Port 64
Suggestions for Attacking Root Port Problems on the Exam 65
Determining the Designated Port on Each LAN Segment 66
Suggestions for Attacking Designated Port Problems on the Exam 67
STP Convergence 68
Troubleshooting EtherChannel 68
Incorrect Options on the channel-group Command 68
Configuration Checks Before Adding Interfaces to EtherChannels 70
Exam Preparation Tasks 73

Chapter 3 Troubleshooting LAN Switching 77
"Do I Know This Already?" Quiz 77
Foundation Topics 78
Generalized Troubleshooting Methodologies 78
Analyzing and Predicting Normal Network Operation 79
Data Plane Analysis 79
Control Plane Analysis 81
Predicting Normal Operations: Summary of the Process 81
Problem Isolation 82
Root Cause Analysis 83
Real World Versus the Exams 84

Troubleshooting the LAN Switching Data Plane 84
An Overview of the Normal LAN Switch Forwarding Process 85
Step 1: Confirm the Network Diagrams Using CDP 86
Step 2: Isolate Interface Problems 88
Interface Status Codes and Reasons for Nonworking States 88
The notconnect State and Cabling Pinouts 90
Determining Switch Interface Speed and Duplex 91
Issues Related to Speed and Duplex 92
Step 3: Isolate Filtering and Port Security Problems 94
Step 4: Isolate VLAN and Trunking Problems 98
Ensuring That the Right Access Interfaces Are in the Right VLANs 98
Access VLANs Not Being Defined or Not Being Active 100
Identify Trunks and VLANs Forwarded on Those Trunks 100
Troubleshooting Examples and Exercises 102
Troubleshooting Example 1: Find Existing LAN Data Plane Problems 103
Step 1: Verify the Accuracy of the Diagram Using CDP 104
Step 2: Check for Interface Problems 105
Step 3: Check for Port Security Problems 107
Step 4: Check for VLAN and VLAN Trunk Problems 109
Troubleshooting Example 2: Predicting LAN Data Plane Behavior 112
PC1 ARP Request (Broadcast) 113
R1 ARP Reply (Unicast) 116
Exam Preparation Tasks 121

Part I Review 124

Part II: IP Version 4 Routing 129

Chapter 4 Troubleshooting IPv4 Routing Part I 131
"Do I Know This Already?" Quiz 131
Foundation Topics 132
Predicting Normal IPv4 Routing Behavior 132
Host IPv4 Routing Logic 132
Routing Logic Used by IPv4 Routers 133
IP Routing Logic on a Single Router 134
IP Routing from Host to Host 135
Building New Data Link Headers Using ARP Information 136

Problem Isolation Using the ping Command 137
Ping Command Basics 138
Strategies and Results When Testing with the ping Command 139
Testing Longer Routes from Near the Source of the Problem 139
Using Extended Ping to Test the Reverse Route 142
Testing LAN Neighbors with Standard Ping 144
Testing LAN Neighbors with Extended Ping 145
Testing WAN Neighbors with Standard Ping 145
Using Ping with Names and with IP Addresses 146
Problem Isolation Using the traceroute Command 147
traceroute Basics 147
How the traceroute Command Works 148
Standard and Extended traceroute 150
Using traceroute to Isolate the Problem to Two Routers 151
Exam Preparation Tasks 154

Chapter 5 Troubleshooting IPv4 Routing Part II 157
"Do I Know This Already?" Quiz 157
Foundation Topics 158
Problems Between the Host and the Default Router 158
Root Causes Based on a Host's IPv4 Settings 158
Ensure IPv4 Settings Correctly Match 158
Mismatched Masks Impact Route to Reach Subnet 160
Typical Root Causes of DNS Problems 161
Wrong Default Router IP Address Setting 163
Root Causes Based on the Default Router's Configuration 163
Mismatched VLAN Trunking Configuration with Router on a Stick 163
DHCP Relay Issues 166
Router LAN Interface and LAN Issues 167
Problems with Routing Packets Between Routers 169
IP Forwarding by Matching the Most Specific Route 170
*Using **show ip route** and Subnet Math to Find the Best Route 170*
*Using **show ip route** address to Find the Best Route 172*
***show ip route** Reference 172*
Routing Problems Caused by Incorrect Addressing Plans 174
Recognizing When VLSM Is Used or Not 174
Overlaps When Not Using VLSM 174

Overlaps When Using VLSM 176
Configuring Overlapping VLSM Subnets 177
Router WAN Interface Status 178
Filtering Packets with Access Lists 178
Exam Preparation Tasks 181

Chapter 6 Creating Redundant First-Hop Routers 183
"Do I Know This Already?" Quiz 183
Foundation Topics 186
FHRP Concepts 186
The Need for Redundancy in Networks 186
The Need for a First Hop Redundancy Protocol 188
The Three Solutions for First-Hop Redundancy 189
HSRP Concepts 190
HSRP Failover 191
HSRP Load Balancing 192
GLBP Concepts 193
FHRP Configuration and Verification 195
Configuring and Verifying HSRP 195
Configuring and Verifying GLBP 198
Exam Preparation Tasks 202

Chapter 7 Virtual Private Networks 205
"Do I Know This Already?" Quiz 205
Foundation Topics 207
VPN Fundamentals 207
IPsec VPNs 209
SSL VPNs 211
GRE Tunnels 212
GRE Tunnel Concepts 212
Routing over GRE Tunnels 213
GRE Tunnels over the Unsecured Network 214
Configuring GRE Tunnels 216
Verifying a GRE Tunnel 218
Exam Preparation Tasks 221

Part II Review 224

Part III: IP Version 4 Routing Protocols 229

Chapter 8 Implementing OSPF for IPv4 231

"Do I Know This Already?" Quiz 231

Foundation Topics 234

OSPF Protocols and Operation 234

OSPF Overview 234

Becoming Neighbors and Exchanging the LSDB 235

Agreeing to Become Neighbors 236

Fully Exchanging LSAs with Neighbors 237

Maintaining Neighbors and the LSDB 238

Using Designated Routers on Ethernet Links 239

Scaling OSPF Using Areas 240

OSPF Areas 241

How Areas Reduce SPF Calculation Time 242

OSPF Area Design Advantages 243

Link-State Advertisements 244

Router LSAs Build Most of the Intra-Area Topology 245

Network LSAs Complete the Intra-Area Topology 245

LSAs in a Multi-Area Design 247

Calculating the Best Routes with SPF 248

Administrative Distance 250

OSPF Configuration and Verification 251

OSPFv2 Configuration Overview 251

Multi-Area OSPFv2 Configuration Example 252

Single-Area Configurations 254

Multi-Area Configuration 255

Verifying the Multi-Area Configuration 256

Verifying the Correct Areas on Each Interface on an ABR 256

Verifying Which Router Is DR and BDR 257

Verifying the Number and Type of LSAs 258

Verifying OSPF Routes 259

OSPF Metrics (Cost) 259

Setting the Cost Based on Interface Bandwidth 260

The Need for a Higher Reference Bandwidth 261

OSPF Load Balancing 262

Exam Preparation Tasks 263

Chapter 9 Understanding EIGRP Concepts 267

"Do I Know This Already?" Quiz 267

Foundation Topics 269

EIGRP and Distance Vector Routing Protocols 269

Introduction to EIGRP 269

Basic Distance Vector Routing Protocol Features 271

The Concept of a Distance and a Vector 271

Full Update Messages and Split Horizon 273

Route Poisoning 275

EIGRP as an Advanced DV Protocol 276

EIGRP Sends Partial Update Messages, As Needed 276

EIGRP Maintains Neighbor Status Using Hello 276

Summary of Interior Routing Protocol Features 277

EIGRP Concepts and Operation 278

EIGRP Neighbors 278

Exchanging EIGRP Topology Information 279

Calculating the Best Routes for the Routing Table 280

The EIGRP Metric Calculation 280

An Example of Calculated EIGRP Metrics 281

Caveats with Bandwidth on Serial Links 283

EIGRP Convergence 284

Feasible Distance and Reported Distance 284

EIGRP Successors and Feasible Successors 285

The Query and Reply Process 287

Exam Preparation Tasks 288

Chapter 10 Implementing EIGRP for IPv4 291

"Do I Know This Already?" Quiz 291

Foundation Topics 294

Core EIGRP Configuration and Verification 294

EIGRP Configuration 294

Configuring EIGRP Using a Wildcard Mask 296

Verifying EIGRP Core Features 296

Finding the Interfaces on Which EIGRP is Enabled 297

Displaying EIGRP Neighbor Status 300

Displaying the IPv4 Routing Table 301

EIGRP Metrics, Successors, and Feasible Successors 302
Viewing the EIGRP Topology Table 303
Finding Successor Routes 305
Finding Feasible Successor Routes 306
Convergence Using the Feasible Successor Route 308
Examining the Metric Components 310
Other EIGRP Configuration Settings 311
Load Balancing Across Multiple EIGRP Routes 311
Tuning the EIGRP Metric Calculation 313
Autosummarization and Discontiguous Classful Networks 314
Automatic Summarization at the Boundary of a Classful Network 314
Discontiguous Classful Networks 315
Exam Preparation Tasks 318

Chapter 11 Troubleshooting IPv4 Routing Protocols 323
"Do I Know This Already?" Quiz 323
Foundation Topics 324
Perspectives on Troubleshooting Routing Protocol Problems 324
Interfaces Enabled with a Routing Protocol 325
EIGRP Interface Troubleshooting 327
Examining Working EIGRP Interfaces 327
Examining the Problems with EIGRP Interfaces 330
OSPF Interface Troubleshooting 332
Neighbor Relationships 335
EIGRP Neighbor Verification Checks 337
EIGRP Neighbor Troubleshooting Example 338
OSPF Neighbor Troubleshooting 339
Finding Area Mismatches 341
Finding Duplicate OSPF Router IDs 342
Finding OSPF Hello and Dead Timer Mismatches 343
Other OSPF Issues 345
Mismatched OSPF Network Types 345
Mismatched MTU Settings 346
Exam Preparation Tasks 348

Part III Review 352

Part IV: Wide-Area Networks 357

Chapter 12 Implementing Point-to-Point WANs 359

"Do I Know This Already?" Quiz 359

Foundation Topics 362

Leased Line WANs with HDLC 362

Layer 1 Leased Lines 363

The Physical Components of a Leased Line 363

Leased Lines and the T-Carrier System 365

The Role of the CSU/DSU 367

Building a WAN Link in a Lab 367

Layer 2 Leased Lines with HDLC 368

Configuring HDLC 370

Leased-Line WANs with PPP 373

PPP Concepts 373

PPP Framing 374

PPP Control Protocols 374

PPP Authentication 375

Configuring PPP 376

CHAP Configuration and Verification 377

Troubleshooting Serial Links 378

Troubleshooting Layer 1 Problems 379

Troubleshooting Layer 2 Problems 380

Keepalive Failure 381

PAP and CHAP Authentication Failure 382

Troubleshooting Layer 3 Problems 383

Exam Preparation Tasks 386

Chapter 13 Understanding Frame Relay Concepts 389

"Do I Know This Already?" Quiz 389

Foundation Topics 392

Frame Relay Overview 392

Virtual Circuits 394

LMI and Encapsulation Types 396

Frame Relay Encapsulation and Framing 397

Frame Relay Addressing 398

Frame Relay Local Addressing 398

Frame Forwarding with One DLCI Field 399

Network Layer Addressing with Frame Relay 401
Frame Relay Layer 3 Addressing: One Subnet Containing All Frame Relay DTEs 401
Frame Relay Layer 3 Addressing: One Subnet Per VC 402
Frame Relay Layer 3 Addressing: Hybrid Approach 404
Exam Preparation Tasks 406

Chapter 14 Implementing Frame Relay 409
"Do I Know This Already?" Quiz 409
Foundation Topics 412
Frame Relay Configuration and Verification 412
Planning a Frame Relay Configuration 412
Configuring Using Physical Interfaces and One IP Subnet 413
Configuring the Encapsulation and LMI 415
Frame Relay Address Mapping 416
Inverse ARP 419
Static Frame Relay Mapping 420
Configuring Point-to-Point Subinterfaces 421
Verifying Point-to-Point Frame Relay 424
Configuring with Multipoint Subinterfaces 426
OSPF Issues on Frame Relay Multipoint and Physical Interfaces 429
Frame Relay Troubleshooting 430
A Suggested Frame Relay Troubleshooting Process 430
Layer 1 Issues on the Access Link (Step 1) 432
Layer 2 Issues on the Access Link (Step 2) 432
PVC Problems and Status (Step 3) 433
Find the Connected Subnet and Outgoing Interface (Steps 3a and 3b) 435
Find the PVCs Assigned to That Interface (Step 3c) 435
Determine Which PVC Is Used to Reach a Particular Neighbor (Step 3d) 437
PVC Status 437
Subinterface Status 439
Frame Relay Mapping Issues (Step 4) 440
End-to-End Encapsulation (Step 5) 441
Mismatched Subnet Numbers (Step 6) 441
Exam Preparation Tasks 442

Chapter 15 Identifying Other Types of WANs 445
"Do I Know This Already?" Quiz 445
Foundation Topics 447
Private WANs to Connect Enterprises 447
Leased Lines 447
Frame Relay 449
Ethernet WANs 449
MPLS 451
VSAT 452
Public WANs and Internet Access 453
Internet Access (WAN) Links 453
Dial Access with Modems and ISDN 454
Digital Subscriber Line 456
Cable Internet 457
Mobile Phone Access with 3G/4G 459
PPP over Ethernet 460
PPP over Ethernet Concepts 460
PPP over Ethernet Configuration 461
Exam Preparation Tasks 463

Part IV Review 464

Part V: IP Version 6 469

Chapter 16 Troubleshooting IPv6 Routing 471
"Do I Know This Already?" Quiz 471
Foundation Topics 472
Normal IPv6 Operation 472
Unicast IPv6 Addresses and IPv6 Subnetting 472
Assigning Addresses to Hosts 475
Stateful DHCPv6 475
Stateless Address Autoconfiguration 476
Router Address and Static Route Configuration 477
Configuring IPv6 Routing and Addresses on Routers 477
IPv6 Static Routes on Routers 478
Verifying IPv6 Connectivity 479
Verifying Connectivity from IPv6 Hosts 479
Verifying IPv6 from Routers 481

Troubleshooting IPv6 483
Pings from the Host Work Only in Some Cases 484
Pings Fail from a Host to Its Default Router 486
Problems Using Any Function That Requires DNS 487
Host Is Missing IPv6 Settings: Stateful DHCP Issues 488
Host Is Missing IPv6 Settings: SLAAC Issues 489
Traceroute Shows Some Hops, But Fails 490
Routing Looks Good, But Traceroute Still Fails 492
Exam Preparation Tasks 494

Chapter 17 Implementing OSPF for IPv6 499
"Do I Know This Already?" Quiz 499
Foundation Topics 502
OSPFv3 Configuration 502
OSPFv3 ICND1 Configuration Review 502
Example Multi-Area OSPFv3 Configuration 503
Single Area Configuration on the Three Internal Routers 504
Adding Multi-Area Configuration on the Area Border Router 506
Other OSPFv3 Configuration Settings 507
Setting OSPFv3 Interface Cost to Influence Route Selection 507
OSPF Load Balancing 508
Injecting Default Routes 508
OSPF Concepts, Verification, and Troubleshooting 509
OSPFv3 Interfaces 511
Verifying OSPFv3 Interfaces 511
Troubleshooting OSPFv3 Interfaces 512
OSPFv3 Neighbors 513
Verifying OSPFv3 Neighbors 513
Troubleshooting OSPFv3 Neighbors 514
OSPFv3 LSDB and LSAs 517
Verifying OSPFv3 LSAs 517
Troubleshooting OSPFv3 LSAs 519
OSPFv3 Metrics and IPv6 Routes 520
Verifying OSPFv3 Interface Cost and Metrics 520
Troubleshooting IPv6 Routes Added by OSPFv3 523
Exam Preparation Tasks 525

Chapter 18 Implementing EIGRP for IPv6 529

"Do I Know This Already?" Quiz 529

Foundation Topics 532

EIGRPv6 Configuration 532

EIGRPv6 Configuration Basics 532

EIGRPv6 Configuration Example 533

Other EIGRPv6 Configuration Settings 536

Setting Bandwidth and Delay to Influence EIGRPv6 Route Selection 536

EIGRP Load Balancing 537

EIGRP Timers 538

EIGRPv6 Concepts, Verification, and Troubleshooting 538

EIGRPv6 Interfaces 539

EIGRPv6 Neighbors 541

EIGRPv6 Topology Database 543

EIGRPv6 IPv6 Routes 545

Exam Preparation Tasks 547

Part V Review 550

Part VI: Network Management 555

Chapter 19 Managing Network Devices 557

"Do I Know This Already?" Quiz 557

Foundation Topics 560

Simple Network Management Protocol 560

Describing SNMP 560

The Management Information Base 562

Configuring SNMP Version 2c 563

SNMP Version 3 565

System Message Logging (Syslog) 566

An Overview of System Message Logging 566

System Message Format 567

System Message Severity Levels 567

Configuring and Verifying Syslog 568

Using a Syslog Server 569

NetFlow 570

An Overview of NetFlow 570

Network Flows 571

Configuring NetFlow 572

Verifying and Using NetFlow 573
The NetFlow Collector 575
Exam Preparation Tasks 576

Chapter 20 Managing IOS Files 579
"Do I Know This Already?" Quiz 579
Foundation Topics 581
Managing Cisco IOS Files 581
Upgrading a Cisco IOS Software Image into Flash Memory 581
The Cisco IOS Software Boot Sequence 584
The Three Router Operating Systems 585
The Configuration Register 586
How a Router Chooses Which OS to Load 586
Recovering If the IOS Does Not Load 588
Verifying the IOS Image Using the ***show version*** *Command 589*
Password Recovery 591
The General Ideas Behind Cisco Password Recovery/Reset 591
A Specific Password Reset Example 592
Managing Configuration Files 595
Configuration File Basics 595
Copying and Erasing Configuration Files 597
Initial Configuration (Setup Mode) 599
Exam Preparation Tasks 601

Chapter 21 Managing IOS Licensing 605
"Do I Know This Already?" Quiz 605
Foundation Topics 607
IOS Packaging 607
IOS Images per Model, Series, and per Software Version/Release 607
Original Packaging: One IOS Image per Feature Set Combination 608
New IOS Packaging: One Universal Image with All Feature Sets 609
IOS Software Activation with Universal Images 609
Managing Software Activation with Cisco License Manager 611
Manually Activating Software Using Licenses 612
Example of Manually Activating a License 614
Showing the Current License Status 614
Adding a Permanent Technology Package License 616
Right-to-Use Licenses 618
Exam Preparation Tasks 621

Part VI Review 624

Part VII: Final Review 627

Chapter 22 Final Review 629

Advice About the Exam Event 629

Learn the Question Types Using the Cisco Certification Exam Tutorial 629

Think About Your Time Budget Versus Numbers of Questions 630

A Suggested Time-Check Method 631

Miscellaneous Pre-Exam Suggestions 631

Exam-Day Advice 632

Exam Review 632

Practice Subnetting and Other Math-Related Skills 633

Take Practice Exams 635

Practicing Taking the ICND2 Exam 635

Practicing Taking the CCNA Exam 636

Advice on How to Answer Exam Questions 638

Taking Other Practice Exams 639

Find Knowledge Gaps Through Question Review 640

Practice Hands-On CLI Skills 642

Review Mind Maps from Part Review 643

Do Labs 643

Other Study Tasks 643

Final Thoughts 644

Part VIII: Appendixes 647

Appendix A Numeric Reference Tables 649

Appendix B ICND2 Exam Updates 657

Glossary 687

Index 706

DVD-only Appendixes

Appendix C Answers to the "Do I Know This Already?" Quizzes

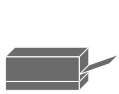
Appendix D Memory Tables

Appendix E Memory Tables Answer Key

Appendix F Mind Map Solutions

Appendix G Study Planner

Icons Used in This Book


Printer


PC

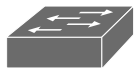

Laptop


Server


Phone

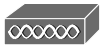

IP Phone


Router


Switch


Frame Relay Switch


Cable Modem

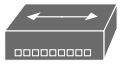

Access Point


ASA


DSLAM


WAN Switch


CSU/DSU


Hub


PIX Firewall


Bridge


Layer 3 Switch


Network Cloud

Ethernet Connection


Serial Line

Virtual Circuit


Ethernet WAN

Wireless

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 Exams

Congratulations! If you're reading far enough to look at this book's Introduction, you've probably already decided to go for your Cisco certification. 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.)

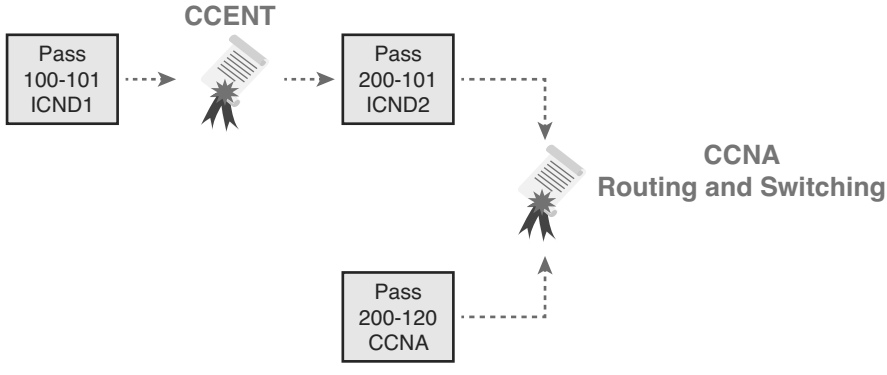


Figure I-1 *Cisco Entry-Level Certifications and Exams*

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 Exam 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
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

Chapter	IP Routing Technologies
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
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

Chapter	IP Services
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
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

Chapter	Network Device Security
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
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
8, 17	**Configure and verify OSPF (single area)**

Chapters	IP Routing Technologies
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
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**

Chapters	Troubleshooting
12	Serial interfaces
12	PPP
14	Frame relay
19	**Monitor NetFlow statistics**
2	**Troubleshoot etherchannel problems**

Table I-12 ICND2 Exam Topics: WAN Technologies

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**
15	**Implement and troubleshoot PPPoE**

CCNA Exam Topics

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.

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*, 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:

- **"Do I Know This Already?" quizzes:** Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying 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.
- **Exam Preparation Tasks:** At the end of the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" 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:
  - **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 Exam Preparation Tasks 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.

- **Review DIKTA Questions:** Although you have already seen the DIKTA 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 DIKTA 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 the Chapter Review tasks and repeat any that you think might help your 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*.)
- **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:** If you are interested in obtaining an eBook version of this title, we have included a special offer on a coupon card inserted in the DVD sleeve in the back of the book. This offer allows you to purchase the *Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide Premium Edition eBook and Practice Test* at a 70 percent discount off the list price. In addition to three versions of the eBook, PDF (for reading on your computer), EPUB (for reading on your tablet, mobile device, or Nook or other eReader), and Mobi (the native Kindle version), you also receive additional practice test questions and enhanced practice test features.
- **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-to-the-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 Appendixes

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 the 'Do I Know This Already?' Quizzes"** 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 activation code for the practice exam associated with this book. *Do not lose the activation code.*

NOTE Also on this same piece of paper, on the opposite side from the exam activation code, you will find a one-time-use coupon code that gives you 70 percent off the purchase of the *Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Premium Edition eBook and Practice Test*.

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 another Pearson product, you do not need to reinstall the software. Instead, just launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the DVD sleeve. The following steps outline the installation process:

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 shortcut 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 from paper inside the cardboard DVD holder in the back of the book. When it is entered, 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

This book includes an activation code that allows you to load a set of practice questions. The 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 six different "exams," or six different sets of questions, as listed in Figure I-2.

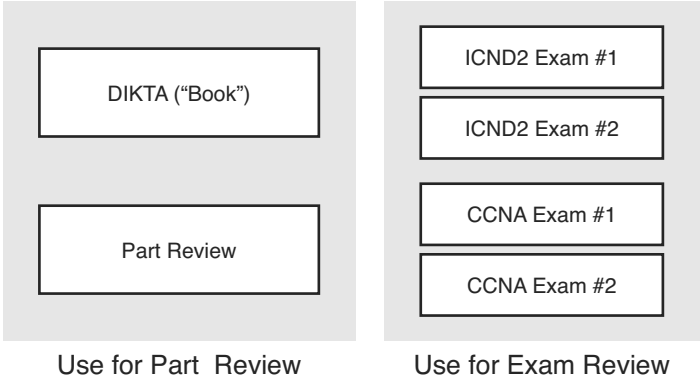


Figure I-2 *PCPT Exams/Exam Databases and When to Use Them*

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 DIKTA questions 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 DIKTA Questions by Part

Each Part Review asks you to repeat the DIKTA 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 DIKTA (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 DIKTA questions from the beginning 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. DIKTA 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 DIKTA/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.

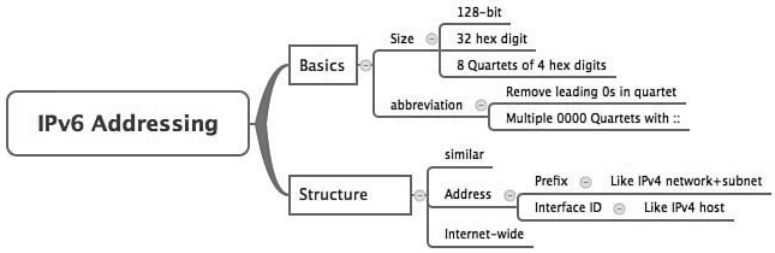


Figure I-3 *Sample Mind Map*

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* 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.

This page intentionally left blank

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

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.

"Do I Know This Already?" Quiz

The troubleshooting chapters of this book pull in concepts from many other chapters, including some chapters in *Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide*. They also show you how to approach some of the more challenging questions on the CCNA exams. Therefore, it is useful to read these chapters regardless of your current knowledge level. For these reasons, the troubleshooting chapters do not include a "Do I Know This Already?" quiz. However, if you feel particularly confident about troubleshooting IP routing features covered in this book and *Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide*, feel free to move to the "Exam Preparation Tasks" section near the end of this chapter to bypass the majority of the chapter.

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.

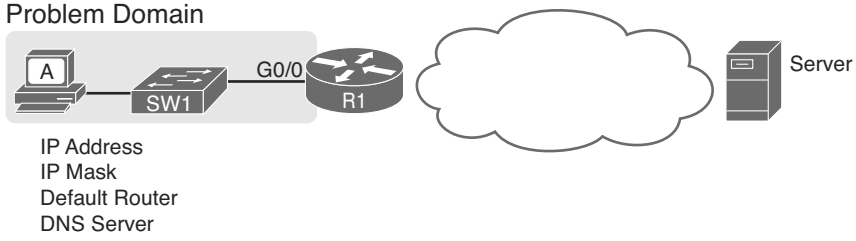


Figure 5-1 *Focus of the Discussions in This Section of the Chapter*

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.

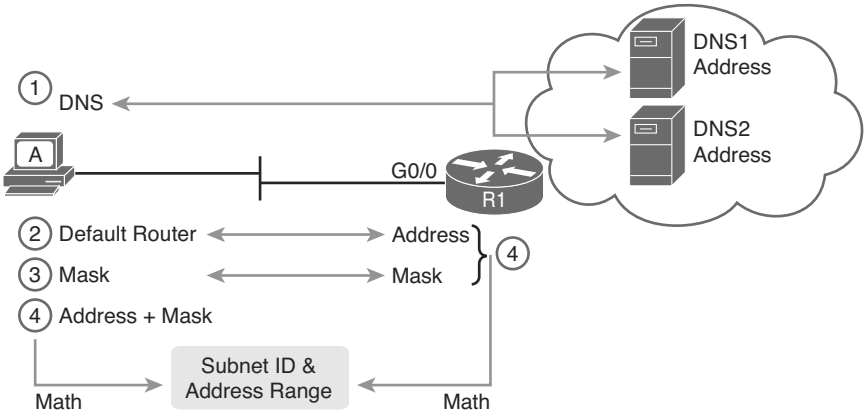


Figure 5-2 *Host IPv4 Settings Compared to What the Settings Should Match*

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.

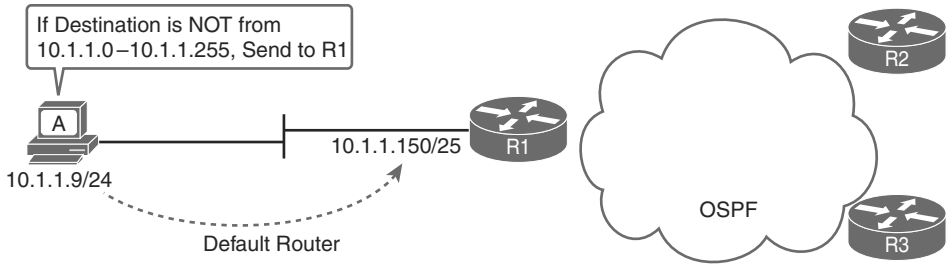


Figure 5-3 *Mismatched Subnet Calculations Appear Workable from Host Toward Network*

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
end
```

```
R1# show ip route connected
! Legend omitted for brevity

      10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
C        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.

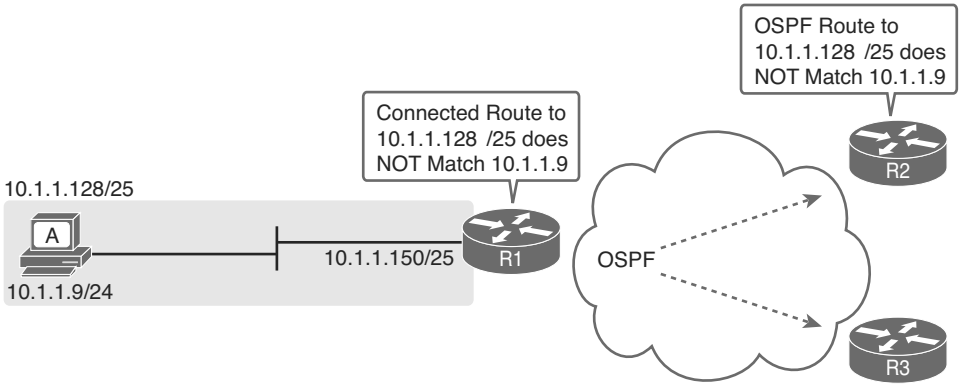


Figure 5-4 *Routers Have No Route That Matches Host A's 10.1.1.9 Address*

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.

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:

Key Topic

- 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.

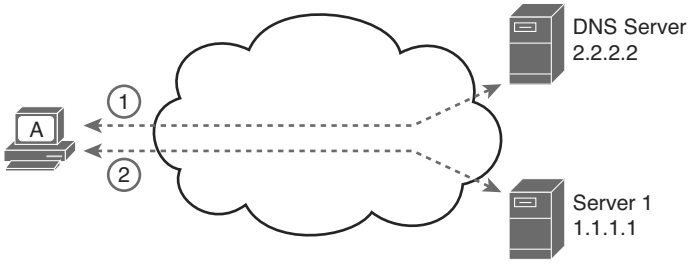


Figure 5-5 *DNS Name Resolution Packets Flow First; Then Packets to the Real Server*

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.)

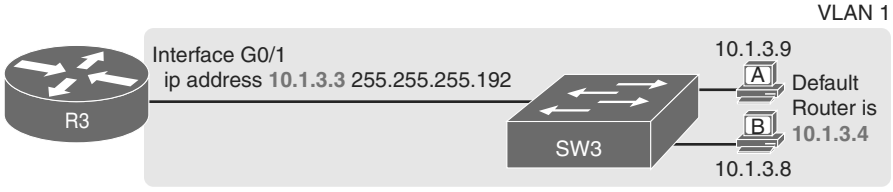


Figure 5-6 *Incorrect Default Router Setting on Hosts A and B*

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 subinterface.
- **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:

Key Topic

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.

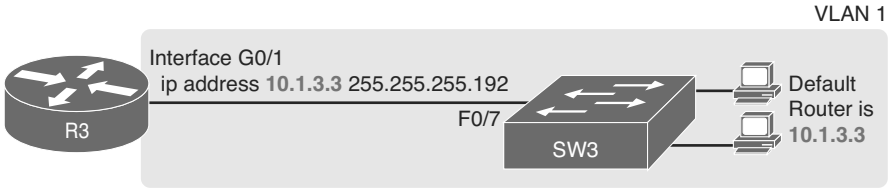


Figure 5-7 *Router IP Address Configuration, Without Trunking*

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.

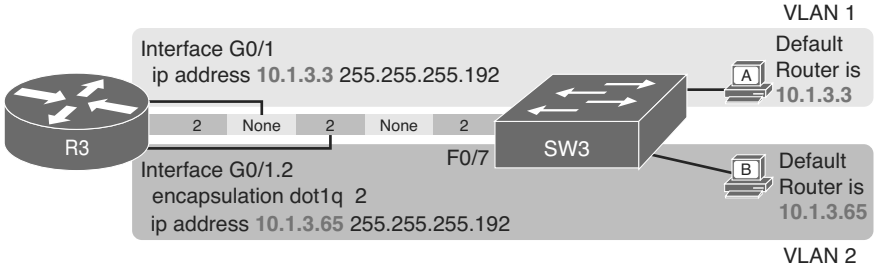


Figure 5-8 *Router IP Address Configuration, with ROAS, and Native VLAN 1*

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

Key Topic

- 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 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.

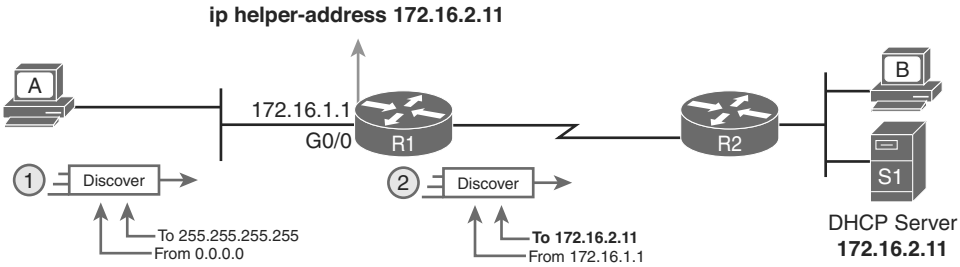


Figure 5-9 *IP Helper Address Effect*

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

Key Topic

- 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.

5

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.

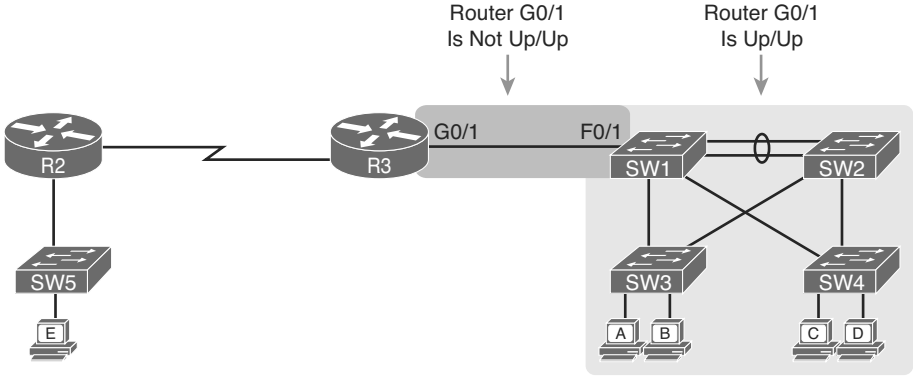


Figure 5-10 *Where to Look for Problems Based on Router LAN Interface Status*

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.

Key Topic

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 **speed** interface subcommand to set the speed, but to different speeds.	down/down
Shutdown	The router interface has been configured with the **shutdown** 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 cable	The router has no cable installed, or the cable pinouts are incorrect.*	down/down

* 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.

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

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

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:

Key Topic

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
O       172.16.1.1/32 [110/50] via 172.16.25.2, 00:00:04, Serial0/1/1
O       172.16.1.0/24 [110/100] via 172.16.25.129, 00:00:09, Serial0/1/0
O       172.16.0.0/22 [110/65] via 172.16.25.2, 00:00:04, Serial0/1/1
O       172.16.0.0/16 [110/65] via 172.16.25.129, 00:00:09, Serial0/1/0
O       0.0.0.0/0 [110/129] via 172.16.25.129, 00:00:09, Serial0/1/0
!
```

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.

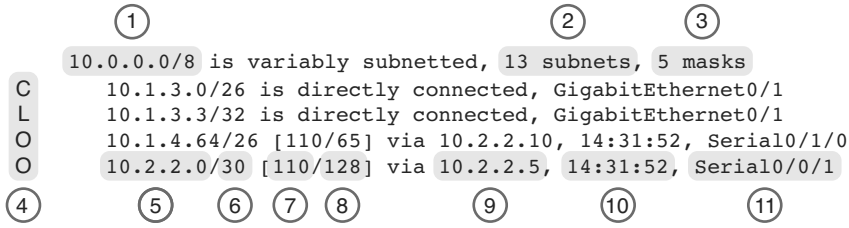


Figure 5-11 **show ip route** *Command Output Reference*

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. *O* is for OSPF, *D* for EIGRP, *C* for Connected, *S* for Static, and *L* 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.

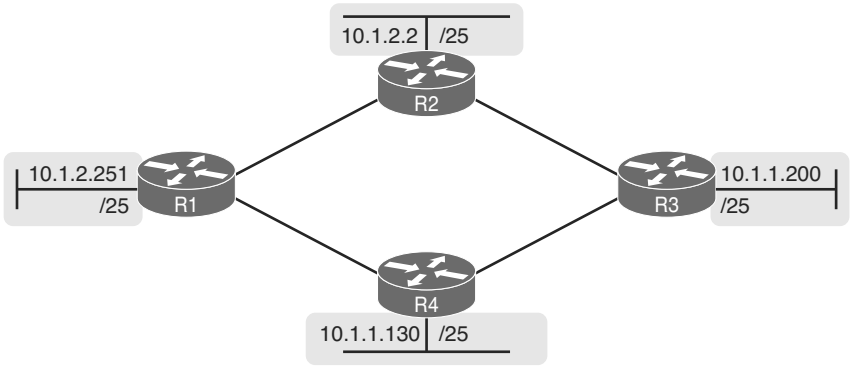


Figure 5-12 *IP Addresses on LAN Interfaces, with One Mask (/25) in Network 10.0.0.0*

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.

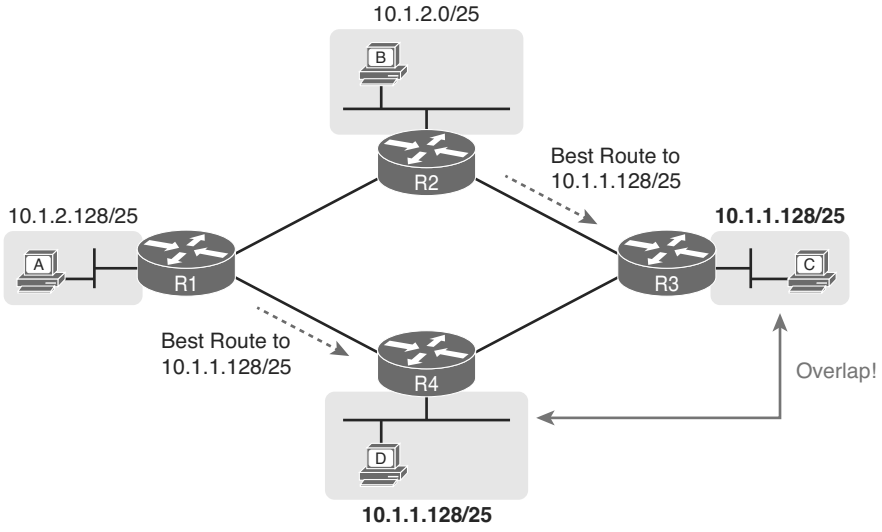


Figure 5-13 *Subnet IDs Calculated from Figure 5-12*

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, non-overlapping 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.

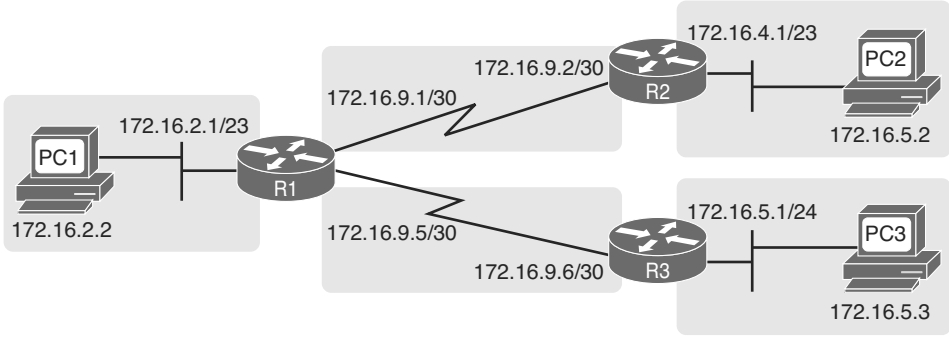


Figure 5-14 *VLSM IP Addressing Plan in Network 172.16.0.0*

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).

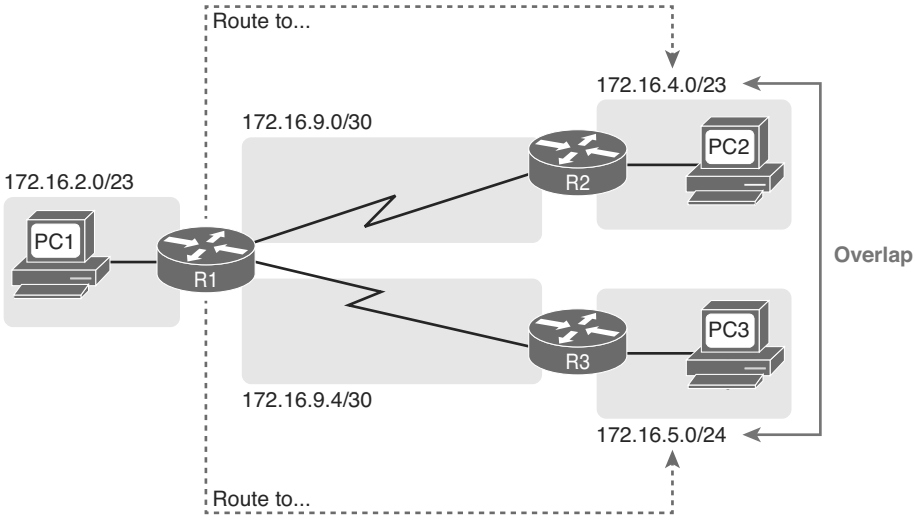


Figure 5-15 *A VLSM Overlap Example, But with Different Subnet IDs*

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:

Key Topic

- **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 S0/0/1** 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

Exam Preparation Tasks

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.

Key Topic

Table 5-4 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
List	Two root causes of DNS problems.	162
List	The rules for configuring ROAS.	164
List	Items to verify for switch trunking configuration to match a router's ROAS configuration.	166
List	Conditions that must be true for DHCP messages to be able to flow from a client to a DHCP server.	167
Table 5-1	Common reasons why router LAN interfaces are not up/up.	169
Definition	When more than one route matches a packet's destination address, the router uses the "best" (most specific) route.	170
List	Types of overlapping IP address configuration issues that IOS can and cannot recognize.	177

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 and reverse route

This page intentionally left blank

Index

Symbols

3DES (Triple DES), 211

3G mobile phone access, 459-460

4G mobile phone access, 459-460

A

ABR (Area Border Router), 242

access control lists (ACLs), 178-180, 673-676

access interface VLAN assignments, checking, 109

access links

AR (access rate), 393

Frame Relay, 393

Layer 1 issues, 432

Layer 2 issues, 432

access rate (AR), 393

access VPNs (virtual private networks), 209

ACLs (access control lists), 178-180, 673-676

activating IOS software, 609-610

Cisco License Manager (CLM), 611

manual activation process, 612-617

right-to-use licenses, 618-620

active/passive model, 190

active/standby model, 190

active virtual gateway (AVG), 193

active VLANs, checking for, 110

AD (administrative distance), 250-251

Adaptive Security Appliances (ASA), 209

address mapping (Frame Relay), 416-419

Inverse ARP, 419-420

static mapping, 420-421

Address Resolution Protocol. *See* ARP

addressing

Frame Relay addressing

DLCI (data link connection identifiers), 398-401

frame forwarding, 400

Layer 3 addressing, 401-405

unicast IPv6 addresses, 472-474

adjacent OSPFv2 neighbors, 240

administrative distance (AD), 250-251

ADSL (asymmetric DSL), 457

AES (Advanced Encryption Standard), 211

alternate (root) ports, 659-660

anti-replay, 207

Area Border Router (ABR), 242

areas (OSPF)

design advantages, 243

design rules, 241-242

design terminology, 242

explained, 240-241

intra-area topology, 245-247
multi-area design, 247-248
multi-area OSPFv2
configuring, 252-256
verifying, 256-259
reducing SPF calculation time with, 242-243
single-area OSPF, 240
single-area OSPFv2, 254-255
ARP (Address Resolution Protocol)
Inverse ARP, 419-420
replies (unicast), forwarding path of, 116-120
requests (broadcast), forwarding path of, 113-116
sample ARP process, 137
ASA (Adaptive Security Appliances), 209
ASN (autonomous system number), 279
asymmetric DSL (ADSL), 457
authentication
PAP/CHAP authentication, 382-383
PPP (Point-to-Point Protocol), 375-376
authNoPriv security level, 565
authPriv security level, 565
auto-cost reference-bandwidth command, 261, 264, 508, 526
autonomous system number (ASN), 279
autosummarization
discontiguous classful networks, 315-317
example of, 314-315
auto-summary command, 294, 315, 319
AVG (active virtual gateway), 193

B

backbone area, 242
backbone routers, 242
backup (designated) ports, 661-662
backup DRs (BDRs), 239, 257
balancing load
EIGRPv4, 311-313
EIGRPv6, 537
HSRP (Hot Standby Router Protocol), 192
OSPFv2 (Open Shortest Path First version 2), 262
PSVT+ (Per-VLAN Spanning Tree Plus), 48
bandwidth
EIGRPv4 metric calculation, 283-284
EIGRPv6 settings, 536-537
reference bandwidth, 261
bandwidth command, 260, 264, 283, 307, 313, 319, 371, 387, 443, 508, 526, 533, 548
Basic Rate Interface (BRI), 455
BDRs (backup DRs), 239, 257
BID (bridge ID), 27, 48-49
binary-to-hexadecimal conversion, 652
blocking state (STP), 24-26
boot sequence of Cisco IOS Software, 584-585
configuration register, 586
IOS image verification, 589-591
OS selection process, 586-588
recovery if IOS does not load, 588-589
three router operating systems, 585
boot system command, 586-587, 601
boot system flash command, 588, 601
boot system rom command, 601

boot system tftp command, 588
BPDU (bridge protocol data units), 27
BPDU Guard, 38, 56-58
brain dumps, 644
BRI (Basic Rate Interface), 455
bridge ID (BID), 27, 48-49
bridge protocol data units (BPDU), 27
broadcast storms, 22-24
broadcasts
ARP requests, forwarding path of, 113-116
forwarding in VLAN 3, 115-116
ignoring, 114-115

C

Cable Internet, 457-458
cable TV (CATV), 458
cabling pinouts for LAN switches, 90
calculating
powers of 2, 653
routes with EIGRP (Enhanced Interior Gateway Routing Protocol)
bandwidth issues, 283-284
example, 281-283
FD (feasible distance), 284-285
metric calculation, 280-281
RD (reported distance), 284-285
CATV (cable TV), 458
CCNA practice exams, 636-637
CDP (Cisco Discovery Protocol), 86-88, 104-105
cdp enable command, 88
cdp run command, 88
Challenge Handshake Authentication Protocol. *See* CHAP
channel-group command, 58-61, 68-70, 74
Channel service unit/data service unit. *See* CSU/DSU
CHAP (Challenge Handshake Authentication Protocol), 460
configuring, 377-378
troubleshooting, 382-383
checking
active interface VLAN assignments, 109
for active VLANs, 110
choosing
DPs (designated ports), 31-32
RPs (root ports), 29-31
CIR (committed information rate), 394
circuits
PVC (permanent virtual circuits), 393, 433-440
SVC (switched virtual circuits), 393
VC (virtual circuits)
explained, 393-396
Layer 3 addressing, 402-403
Cisco Catalyst switches, 95
Cisco Certification Exam Tutorial, 629-630
Cisco Learning Network, 644
Cisco License Manager (CLM), 611
Cisco Prime, 561
Cisco Product License Registration Portal, 613
classful routing protocols, 314
clear ip ospf process command, 235, 265, 343
CLI (command-line interface), 642-643
clients, VPN (virtual private network) clients, 209
CLM (Cisco License Manager), 611
clock rate command, 368-370
clock speed command, 387

collector (NetFlow), 575
committed information rate (CIR), 394
community strings (SNMP), 563
competing routes, 672-673
config-register command, 586, 601
configuration files, 595-597
copying, 597-599
erasing, 597-599
running-config, 596
setup mode, 599
startup-config, 596
configuration register, 586
configuring
BPDU Guard, 56-58
CHAP (Challenge Handshake Authentication Protocol), 377-378
Cisco Catalyst switches, 95
EIGRPv4
basic configuration, 294-295
compared to EIGRPv6, 538-539
convergence, 308-310
feasible successors, 306-308
load balancing, 311-313
maximum-paths, 311-313
metric calculation, 313-314
metric components, 310
successors, 305-306
topology table, viewing, 303-305
variance, 311-313
verifying core features of, 296-302
wildcard masks, 296
EIGRPv6
bandwidth and delay settings, 536-537
basic configuration, 532-533
compared to EIGRPv4, 538-539
configuration commands, 533
example, 533-536
interfaces, 539-541
IPv6 routes, 545-546
load balancing, 537
neighbors, 541-543
overview, 532
timers, 538
topology database, 543-545
EtherChannel
channel-group command options, 68-70
dynamic EtherChannel, 60-61
interface configuration settings, 70-72
manual EtherChannel, 58-60
Frame Relay
address mapping, 416-421
encapsulation, 415-416
fully meshed networks with one IP subnet, 413-415
LMI (Local Management Interface), 415-416
multipoint subinterfaces, 426-429
OSPF (Open Shortest Path First), 429
planning configurations, 412-413
point-to-point subinterfaces, 421-424
self-assessment, 409-411
verification, 424-426
GLBP (Gateway Load Balancing Protocol), 198-201
GRE (generic routing encapsulation) tunnels, 216-218
HDLC (High-level Data Link Control), 370-372

HSRP (Hot Standby Router Protocol), 195-197
IPv6 hosts
router address, 477-478
SLAAC (stateless address autoconfiguration), 476-477
stateful DHCPv6, 475
static routes, 478-479
verifying connectivity, 479-483
NetFlow, 572
OSPFv2 (Open Shortest Path First version 2), 680-683
basic configuration, 251-252
load balancing, 262
multi-area configuration, 252-256
single-area configuration, 254-255
verifying configuration, 256-259
OSPFv3 (Open Shortest Path First version 3)
basic configuration, 502
default routes, 508-509
interface cost, 507-508
load balancing, 508
multi-area configuration, 503-506
single-area configuration, 504-505
overlapping subnets, 177-178
PortFast, 56-58
PPP (Point-to-Point Protocol), 376-377
PPPoE (PPP over Ethernet), 461-462
RSTP (Rapid Spanning Tree Protocol),
identifying STP mode on Catalyst swtiches, 663-666
port roles, 666-667
port states, 667
port types, 668-669
SNMP (Simple Network Management Protocol)
SNMP version 2c, 563-565
SNMP version 3, 565
static routes, 669-671
with competing routes, 672-673
with no competing routes, 671
STP (Spanning Tree Protocol), 46
BID (bridge ID), 48-49
BPDU Guard, 56-58
defaults and configuration options, 49-50
EtherChannel, 58-61
per-VLAN configuration settings, 47-48
per-VLAN costs, 49
port costs, 54
PortFast, 56-58
STP mode, 47
STP port costs, 53-55
switch priority, 54-56
system ID extension, 48-49
verifying STP operation, 50-53
Syslog (System Message Logging), 568-569
confreg command, 592
contiguous classful networks, 316
control plane, 79
control plane analysis, 81
convergence
EIGRP (Enhanced Interior Gateway Routing Protocol)
explained, 284
feasible successors, 308-310
query/reply process, 287
successors, 285-287

STP (Spanning Tree Protocol), 25, 35
delays, 36
troubleshooting, 68
converting
binary to hexadecimal, 652
decimal to binary, 649-651
hexadecimal to binary, 652
copy command, 597-602
copy running-config startup-config command, 586, 593, 597, 602
copy startup-config running-config command, 593, 595, 598, 602
copying
configuration files, 597-599
images into Flash memory, 581-584
CPE (customer premise equipment), 364
CSU/DSU, 367
customer premise equipment (CPE), 364

D

data communications equipment (DCE), 393
Data Encryption Standard (DES), 211
data link connection identifiers (DLCI), 393-394
explained, 398
frame forwarding, 400
frame forwarding with one DLCI field, 399-401
local DLCI, 398-399
data link headers. building, 136-137
data plane, 79
data plane analysis, 79-81
data terminal equipment (DTE), 392-393, 401-402
datak9, 610
Dead Interval timer, 238
debug eigrp fsm command, 320
debug eigrp packets command, 350
debug frame-relay lmi command, 426, 443
debug ip ospf adj command, 341-342, 350
debug ip ospf events command, 350
debug ip ospf hello command, 344, 350
debug ip ospf packet command, 350
debug ipv6 ospf adj command, 513
debug ppp authentication command, 382, 387
debug ppp negotiation command, 387
debug spanning-tree events command, 54, 75
decimal-to-binary conversion, 649-651
dedicated routers (DRs), verifying, 257
default-information originate command, 508-510, 680
default routers, troubleshooting, 158
DHCP Relay, 166-167
DNS problems, 161-162
IP address settings, 163
LAN issues, 167-169
mismatched IPv4 settings, 158-159
mismatched masks, 160-161
mismatched VLAN trunking configuration, 163-166
default routes
OSPFv2, 679-680
OSPFv3, 508-509
delay, EIGRPv6 settings, 536-537
delay command, 313, 319, 533, 548
delivery headers, 215

DES (Data Encryption Standard), 211
description command, 387
designated ports (DPs)
choosing, 31-32
determining, 66
explained, 26
RSTP (Rapid Spanning Tree Protocol), 661-662
strategies for DP exam questions, 67-68
designated routers. *See* DRs
determining
duplex issues, 92-94
root switches, 62-63
RPs (root ports), 63-65
switch interface speed, 91-94
DHCP
Relay, 166-167
stateful DHCP, 488-489
stateful DHCPv6, 475
dial access, 454-456
dialer pool command, 462
Diffusing Update Algorithm (DUAL), 287
digital subscriber line (DSL), 456-457
dir command, 622
discontiguous classful networks, 315-317
distance vector (DV) routing protocols
explained, 271-273
full update messages, 273-274
route poisoning, 275-276
split horizon, 274-275
DLCI (data link connection identifiers)
explained, 398
frame forwarding, 399-401
Frame Relay, 393-394
local DLCI, 398-399
DNS (Domain Name Service)
name resolution, 147
troubleshooting
in IPv4, 161-162
in IPv6, 487
dns-server command, 162
Domain Name Service. *See* DNS
DPs (designated ports)
choosing, 31-32
determining, 66
explained, 26
strategies for DP exam questions, 67-68
DROthers, 239
DRs (designated routers)
on Ethernet links, 239-240
verifying, 257
DSL (digital subscriber line), 456-457
DSLAM (DSL access multiplexer), 457
DTE (data terminal equipment)
access links, 393
Frame Relay, 392-393, 401-402
DUAL (Diffusing Update Algorithm), 287
duplex half command, 92
duplex mismatch, 92-94, 106-107
duplicate OSPF router IDs, finding, 342-343
DV (distance vector) routing protocols
explained, 271-273
full update messages, 273-274
route poisoning, 275-276
split horizon, 274-275
dynamic EtherChannels, configuring, 60-61

E

Echo Requests (ICMP), 151
edge ports, 663
eigrp router-id command, 300, 533, 535, 548
EIGRPv4 (Enhanced Interior Gateway Routing Protocol version 4), 291, 529
advantages of, 270
autosummarization, 314
discontiguous classful networks, 315-317
example of, 314-315
basic configuration, 294-295
compared to EIGRPv6, 538-539
compared to other routing protocols, 271, 277
configuring
feasible successors, 308
maximum-paths, 311-313
variance, 311
convergence, 308-310
explained, 284
query/reply process, 287
successors, 285-287, 308
development of, 269-270
discontiguous classful networks, 315-317
DUAL (Diffusing Update Algorithm), 287
explained, 278
feasible successors, 306-308
hello packets, 276-277
interfaces
examining working interfaces, 327-329
troubleshooting, 325-332
load balancing, 311-313
loop avoidance, 284
metric calculation, 313-314
metric components, 310
neighbors, 278-279
troubleshooting, 335-339
verification checks, 337-338
partial update messages, 276
route calculation
bandwidth issues, 283-284
example, 281-283
FD (feasible distance), 284-285
metric calculation, 280-281
RD (reported distance), 284-285
self-assessment, 267-268, 291-293
Split Horizon issues, 684-686
successors, 305-306
topology table, viewing, 303-305
troubleshooting
interfaces, 325-332
neighbors, 335-339
overview, 324-325
self-assessment, 323
update messages, 279-280
variance, 311-313
verifying core features of, 296-297
interfaces, 297-300
IPv4 routing table, 301-302
neighbor status, 300-301
wildcard masks, 296
EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6)
bandwidth and delay settings, 536-537
basic configuration, 532-533
compared to EIGRPv4, 538-539
configuration commands, 533

configuration example, 533-536
explained, 532
interfaces, 539-541
IPv6 routes, 545-546
load balancing, 537
neighbors, 541-543
self-assessment, 529-531
Split Horizon issues, 684-686
timers, 538
topology database, 543-545
electing root switches via STP (Spanning Tree Protocol), 27-29
emulation, Ethernet, 450
encapsulation
end-to-end, 441
Frame Relay, 397-398, 415-416
encapsulation command, 164, 370, 387, 432
encapsulation frame-relay command, 412-415, 432-433, 443
encapsulation hdlc command, 370
encapsulation ppp command, 376-377
encryption
encryption keys, 210
IPsec, 209-211
end-to-end encapsulation, 441
Enhanced Interior Gateway Routing Protocol. *See* EIGRPv4; EIGRPv6
EoMPLS (Ethernet over MPLS), 450
equal-cost load balancing, 306
erase nvram command, 599, 602
erase startup-config command, 599, 602
erasing configuration files, 597-599
EtherChannel, 37
configuring
channel-group command options, 68-70
dynamic EtherChannel, 60-61
interface configuration settings, 70-72
manual EtherChannel, 58-60
troubleshooting
channel-group command options, 68-70
interface configuration settings, 70-72
Ethernet
EoMPLS (Ethernet over MPLS), 450
Ethernet emulation, 450
Ethernet links, designated routers on, 239-240
Ethernet WANs (wide area networks), 449-451
PPPoE (PPP over Ethernet)
configuring, 461-462
explained, 460-461
eui-64 keyword, 478
exam advice, 629
Cisco Certification Exam Tutorial, 629-630
exam-day advice, 632
Exam Review, 632-633
additional practice exams, 639-640
exam-taking tips, 638-639
math-related skills, 633-634
practice exams, 635-637
hands-on CLI skills, practicing, 642-643
other study tasks, 643-644
pre-exam suggestions, 631-632

Question Review, 640-642
time management, 630-631
Exam Review, 632-633
math-related skills, 633-634
practice exams, 635
additional practice exams, 639-640
CCNA practice exams, 636-637
exam-taking tips, 638-639
ICND2 practice exams, 635-636
Question Review, 640-642
exchanging LSAs with neighbors, 237
extended ping, 142-144
extended traceroute command, 150-151
extranet VPNs (virtual private networks), 208

F

failover, HSRP (Hot Standby Router Protocol), 191-192
FCS (Frame Check Sequence) field, 369
FD (feasible distance), 284-285
feasible successors (EIGRP), 285-287
convergence via, 308-310
creating/viewing, 308
finding, 306-308
FHRP (First Hop Redundancy Protocol)
benefits of, 188-189
comparison of protocols, 678-679
explained, 183, 186, 189-190
GLBP (Gateway Load Balancing Protocol)
active virtual gateway (AVG), 193
configuring, 198-201
explained, 190, 193-195
verifying, 198-201
HSRP (Hot Standby Router Protocol)
configuring, 195-197
explained, 189-190
failover, 191-192
influencing active router choice, 677-678
load balancing, 192
verifying, 195-197
need for network redundancy, 186-188
self-assessment, 183-185
single points of failure, 186-188
VRRP (Virtual Router Redundancy Protocol), 190
filtering
LAN switching, 94-98, 107-109
packets with ACLs (access control lists), 178-180
finding
duplicate OSPF router IDs, 342-343
EIGRPv4 feasible successors, 306-308
EIGRPv4 successors, 305-306
Hello/dead timer mismatches, 343-345
First Hop Redundancy Protocol. ***See*** **FHRP**
Flash memory, upgrading IOS software images into, 581-584
floating static routes, 672
flows (network), 571-572
Forward Delay timers (STP), 34-35
forward routes, 151
forwarding
broadcasts in VLAN 3, 115-116
IP forwarding, troubleshooting, 170-173

LAN switches, 16-17, 85-86
unicasts, 117-119
forwarding state (STP), 24-25
DPs (designated ports)
choosing, 31-32
explained, 26
reasons for, 26
root switches
electing, 27-29
explained, 26
RPs (root ports), 26
Frame Check Sequence (FCS) field, 369
Frame Relay, 389, 449
access links, 393
Layer 1 issues, 432
Layer 2 issues, 432
addressing, 400
AR (access rate), 393
configuring
address mapping, 416-421
encapsulation, 415-416
fully meshed networks with one IP subnet, 413-415
LMI (Local Management Interface), 415-416
multipoint subinterfaces, 426-429
OSPF (Open Shortest Path First), 429
planning configurations, 412-413
point-to-point subinterfaces, 421-424
self-assessment, 409-411
verification, 424-426
DCE (data communications equipment), 393
DLCI (data link connection identifiers), 393-394
explained, 398
frame forwarding, 399-401
local DLCI, 398-399
DTE (data terminal equipment), 392-393, 401-402
encapsulation and framing, 397-398
Layer 3 addressing
hybrid approach, 404-405
one subnet per VC (virtual circuit), 402-403
single subnets containing all DTE, 401-402
LMI (Local Management Interface), 392-397
Multiprotocol Interconnect over Frame Relay, 398
NBMA (nonbroadcast multiaccess) networks, 392-394
overview, 392-397
private WANs, 449
PVC (permanent virtual circuits), 393
subinterface status, 439
troubleshooting, 433-440
self-assessment, 389-391
SVC (switched virtual circuits), 393
troubleshooting, 430
end-to-end encapsulation, 441
Layer 1 issues on access links, 432
Layer 2 issues on access links, 432
mapping issues, 440
mismatched subnet numbers, 441
PVC (permanent virtual circuit) problems, 433-440

self-assessment, 409-411
suggested process, 430-431
VC (virtual circuits)
explained, 393-396
Layer 3 addressing, 402-403
frame-relay interface-dlci command, 413, 416, 423, 428, 439, 443
frame-relay inverse-arp command, 443
frame-relay lmi-type ansi command, 416, 433
frame-relay lmi-type command, 397, 413, 416, 443
frame-relay map command, 413, 416, 421, 439, 443
full-mesh Frame Relay networks, 395
Full neighbor state (OSPF neighbors), 240
full update messages, 273-274
fully adjacent OSPFv2 neighbors, 240
fully meshed networks with one IP subnet, 413-415

G

Gateway Load Balancing Protocol. ***See*** **GLBP (Gateway Load Balancing Protocol)**
gateways, active virtual gateway (AVG), 193
generic routing encapsulation tunnels. ***See*** **GRE tunnels**
GLBP (Gateway Load Balancing Protocol)
active virtual gateway (AVG), 193
comparing with other FHRPs (First Hop Redundancy Protocols), 678-679
configuring, 198-201
explained, 190, 193-195
verifying, 198-201
glbp group ip virtual-ip command, 198
GRE (generic routing encapsulation) tunnels
configuring, 216-218
explained, 212
over unsecured network, 214-216
routing over, 213-214
tunnel interfaces, 213-215
verifying, 218-220

H

HDLC (High-level Data Link Control)
leased-line WANs
building WAN links, 367-368
CSU/DSU, 367
explained, 362
HDLC configuration, 370-372
layer 1 leased lines, 363-368
layer 2 leased lines, 368-370
leased line components, 363-365
T-carrier system, 365-366
overview, 135
Hello/dead timer mismatches, finding, 343-345
Hello Interval timer, 238
hello packets (EIGRP), 276-277
Hello timers (STP), 34-35
hexadecimal-to-binary conversion, 652
high availability campus network design, 188
High-Level Data Link Control (HDLC), 135
host IPv4 routing logic, 132-133
host routes, 384
hostname command, 596
hostnames, pinging, 146-147

hosts
IPv4 routing, troubleshooting
DNS problems, 161-162
IP address settings, 163
mismatched IPv4 settings, 158-159
mismatched masks, 160-161
IPv6 hosts, configuring
router address, 477-478
stateful DHCPv6, 475
stateful SLAAC (stateless address autoconfiguration), 476-477
static routes, 478-479
verifying connectivity, 479-483
Hot Standby Router Protocol. *See* HSRP
how ip protocols command, 327-329
HSRP (Hot Standby Router Protocol)
comparing with other FHRPs (First Hop Redundancy Protocols), 678-679
configuring, 195-197
explained, 189-190
failover, 191-192
influencing active router choice, 677-678
load balancing, 192
verifying, 195-197

I

ICMP
Echo Requests, 151
Time-to-Live Exceeded (TTL Exceeded), 148
ICMP (Internet Control Message Protocol), 138
ICND2 practice exams, 635-636
identifying STP mode on Catalyst switches, 663-666
IDs
BID (bridge ID), configuring, 48-49
system ID extension, configuring, 48-49
IEEE 802.1d. *See* STP (Spanning Tree Protocol)
IEEE 802.1w. *See* RSTP (Rapid Spanning Tree Protocol)
ifconfig command, 480, 496
IFS (IOS File System), 599
ignoring incoming broadcast frame, 114-115
images (IOS)
images per feature set combination, 608
images per model/series, 607
universal images, 609
upgrading into Flash memory, 581-584
inferior hello (STP), 28
infinity, 275
Integrated Services Digital Network (ISDN), 454-456
interarea routes, 242
interface loopback command, 264
interface serial 0/0/0/1 point-to-point command, 423
interface serial command, 443
interface status codes for LAN switches, 88-89
interface tracking, 677-678
interface tunnel command, 215-217
interfaces
EIGRPv4 interfaces, 684-686
finding, 297-300
troubleshooting, 325-332

EIGRPv6 interfaces, 539-541, 684-686
isolating (LAN switching), 88-94, 105-107
cabling pinouts, 90
interface status codes, 88-89
notconnect state, 90
OSPFv2 interfaces, troubleshooting, 325-326, 332-335
OSPFv3 interfaces
troubleshooting, 512-513
verifying, 511
Internal routers, 242
Internet Access Links, 453
Internet Control Message Protocol. ***See*** **ICMP**
Internet Protocol. ***See*** **IP**
intra-area routes, 242
Inverse ARP, Frame Relay address mapping, 419-420
IOS file management
configuration files, 595-597
copying, 597-599
erasing, 597-599
running-config, 596
setup mode, 599
startup-config, 596
IOS software
boot sequence, 584-585
configuration register, 586
IOS image verification, 589-591
OS selection process, 586-588
recovery if IOS does not load, 588-589
three router operating systems, 585
upgrading images into Flash memory, 581-584
password recovery
example, 592-595
explained, 591-592
self-assessment, 579-581
IOS File System (IFS), 599
IOS packaging
explained, 607
images per feature set combination, 608
images per model/series, 607
universal images, 609
IOS software activation, 609-610
boot sequence, 584-585
configuration register, 586
IOS image verification, 589-591
OS selection process, 586-588
recovery if IOS does not load, 588-589
three router operating systems, 585
Cisco License Manager (CLM), 611
images, upgrading into Flash memory, 581-584
manual activation
activation process, 612-613
adding permanent technology package license, 616-617
showing current license status, 614-615
right-to-use licenses, 618-620
self-assessment, 605-606
IP (Internet Protocol)
default router IP address settings
troubleshooting, 163
delivery headers, 215
IP forwarding
troubleshooting, 170-173
ip address command, 159, 177, 190, 216-217, 370

IP addressing
binary-to-hexadecimal conversion, 652
decimal-to-binary conversion, 649-651
hexadecimal-to-binary conversion, 652
IP ARP table, displaying, 676
ipbasek9, 610
ipconfig command, 479, 496
IPCP (IP Control Protocol), 374
ip domain-lookup command, 162
ip flow command, 572
ip flow egress command, 572
ip flow-export command, 572
ip flow-export destination command, 572
ip flow-export source command, 572
ip flow-export version command, 572
ip flow ingress command, 572
ip hello-interval eigrp command, 294, 348, 533
ip helper-address command, 166-167
ip hold-time eigrp command, 294, 319, 348, 533
ip mtu command, 519
ip name-server command, 162
ip ospf cost command, 259-261, 264, 526
ip ospf dead-interval command, 349
ip ospf hello-interval command, 349
ip ospf network point-to-multipoint command, 429
ip ospf subcommand, 681-682
ip route command, 250, 669-672
ip split-horizon eigrp asn command, 686
IPsec VPNs (virtual private networks), 209-211

IPv4 routing
default router IP address settings, troubleshooting, 163
delivery headers, 215
DV (distance vector) routing protocols, 271-273
explained, 271-273
full update messages, 273-274
route poisoning, 275-276
split horizon, 274-275
EIGRPv4 (Enhanced Interior Gateway Routing Protocol version 4), 267
advantages of, 270
autosummarization, 314-317
basic configuration, 294-295
compared to other routing protocols, 271, 277
convergence, 284-287, 308-310
development of, 269-270
discontiguous classful networks, 315-317
DUAL (Diffusing Update Algorithm), 287
explained, 278
feasible successors, 306-308
hello packets, 276-277
load balancing, 311-313
loop avoidance, 284
metric calculation, 313-314
metric components, 310
neighbors, 278-279
partial update messages, 276
route calculation, 280-285
self-assessment, 267-268, 291-293
successors, 305-306
topology table, viewing, 303-305

update messages, 279-280
variance, 311-313
verifying core features of, 296-302
wildcard masks, 296
FHRP (First Hop Redundancy Protocol). *See* FHRP
normal routing behavior, predicting
data link headers, 136-137
host IPv4 routing logic, 132-133
IP routing from host to host, 135
IP routing logic on single router, 134-135
sample ARP process, 137
OSPFv2 (Open Shortest Path First version 2)
AD (administrative distance), 250-251
areas, 240-248
basic configuration, 251-252
compared to OSPFv3, 509-510
compared to other routing protocols, 271, 277
DRs (designated routers), 239-240
explained, 234-235
fully neighbors, 240
load balancing, 262
LSAs (link-state advertisements), 237, 244-248, 258
LSDB (link-state databases), 238-239
metrics, 260-261
multi-area configuration, 252-256
neighbors, 236-240
RID (router ID), 235
self-assessment, 231-233
single-area configuration, 254-255
SPF route calculation, 242-243, 248-250
verifying configuration, 256-259
OSPFv3 (Open Shortest Path First version 3), 499
basic configuration, 502
compared to OSPFv2, 509-510
default routes, 508-509
interface cost, 507-508
interfaces, 511-513
IPv6 routes, 523-524
load balancing, 508
LSAs (link-state advertisements), 517-520
metrics, 520-522
multi-area configuration, 503, 506
neighbors, 513-517
self-assessment, 499-501
single-area configuration, 504-505
problem isolation with ping command
explained, 137-139
hostnames and IP addresses, 146-147
LAN neighbors, testing, 144-145
longer routes, testing, 139-142
reverse routes, testing, 142-144
sample output, 138
WAN neighbors, testing, 145-146
problem isolation with traceroute command
explained, 147-150
extended traceroute, 150-151

isolating problems to two routers, 151-153
sample output, 148
standard traceroute, 150
protocol troubleshooting
duplicate router IDs, 342-343
EIGRP interfaces, 325-332
EIGRP neighbors, 335-339
Hello/dead timer mismatches, 343-345
mismatched MTU settings, 346-347
mismatched network types, 345-346
OSPF area mismatches, 341-342
OSPF interfaces, 325-335
OSPF neighbors, 335-345
overview, 324-325
self-assessment, 323
RIP-2, 271, 277
routing logic
from host to host, 135
on single router, 134-135
routing table, displaying, 301-302
static routes, configuring, 669-673
troubleshooting, 131, 157-158
ACLs (access control lists), 178-180, 673-676
DHCP Relay issues, 166-167
DNS problems, 161-162
IP address settings, 163
IP forwarding, 170-173
LAN issues, 167-169
mismatched IPv4 settings, 158-159
mismatched masks, 160-161
mismatched VLAN trunking configuration, 163-166
normal routing behavior, predicting, 132-137
with ping command, 137-147
router WAN interface status, 178
self-assessment, 131, 157
with show ip route command, 170-173
with traceroute command, 147-153
VLSM, 174-178
ipv6 address command, 477-478, 490, 492, 495
ipv6 dhcp relay command, 489
ipv6 dhcp relay destination command, 495
ipv6 eigrp asn command, 533
ipv6 eigrp command, 535, 541, 548
ipv6 hello-interval eigrp command, 548
ipv6 hold-time eigrp command, 548
ipv6 ospf command, 495
ipv6 ospf cost command, 508
ipv6 ospf hello-interval command, 516
ipv6 router eigrp command, 535, 548
ipv6 router ospf command, 495
IPv6 routing
EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6)
bandwidth and delay settings, 536-537
basic configuration, 532-533
compared to EIGRPv4, 538-539
configuration commands, 533
configuration example, 533-536
EIGRP configuration, 529
explained, 532
interfaces, 539-541

IPv6 routes, 545-546
load balancing, 537
neighbors, 541-543
self-assessment, 529-531
timers, 538
topology database, 543-545
host configuration
router address, 477-478
SLAAC (stateless address auto-configuration), 476-477
stateful DHCPv6, 475
static routes, 478-479
IOS packaging
explained, 607
images per feature set combination, 608
images per model/series, 607
universal images, 609
IOS software activation, 609-610
Cisco License Manager (CLM), 611
manual activation, 612-617
right-to-use licenses, 618-620
self-assessment, 605-606
NetFlow
configuring, 572
explained, 570-571
NetFlow collector, 575
network flows, 571-572
verifying, 573-574
SNMP (Simple Network Management Protocol)
community strings, 563
explained, 560-562
MIB (Management Information Base), 562-563
SNMP version 2c, 563-565
SNMP version 3, 565
traps, 561
subnetting, 472-474
Syslog (System Message Logging)
configuring, 568-569
explained, 566
Syslog server, 569
system message format, 567
system message severity levels, 567-568
verifying, 568-569
troubleshooting, 483-484
DNS issues, 487
ping failures, 484-487
self-assessment, 471
SLAAC issues, 489-490
stateful DHCP, 488-489
traceroute failures, 490-493
unicast IPv6 addresses, 472-474
verifying connectivity
from hosts, 479-480
from routers, 481-483
ipv6 unicast-routing command, 477, 490, 495
ISDN (Integrated Services Digital Network), 454-456
isolating
LAN switching interface problems, 82-83, 88-94, 105-107
cabling pinouts, 90
interface status codes, 88-89
notconnect state, 90
IPv4 routing problems
ping command, 137-147
traceroute command, 147-153
VLAN and trunking problems, 20-21, 98-112

K-L

keepalive command, 443
keepalive failure, troubleshooting, 381

LAN neighbors, testing with ping, 144-145
LAN switching
DPs (designated ports)
choosing, 31-32
explained, 26
overview, 16
root cost, 26
root switches
electing, 27-29
explained, 26
router LAN issues, troubleshooting, 167-169
RPs (root ports)
choosing, 29-31
explained, 26
STP (Spanning Tree Protocol). *See* STP
switch verification, 17
determining VLAN of frames, 19-20
switch reactions to changes with STP, 34-35
verifying trunks, 20-21
viewing MAC address table, 17-19
troubleshooting, 77-78
analyzing/predicting normal operation, 79-82
ARP requests (broadcast), forwarding path of, 113-116
cabling pinouts, 90
control plane analysis, 81
data plane analysis, 79-81
duplex issue, 92-94
exam tips, 84
example of, 109
forwarding process overview, 16-17, 85-86
interface status codes, 88-89
isolate filtering/port security problems, 94-98, 107-109
isolation of interface problems, 88-94, 105-107
isolation of VLAN/trunking problems, 20-21, 98-112
network diagram confirmation via CDP, 86-88, 104-105
notconnect state, 90
problem isolation, 82-83
R1 ARP Reply (unicast), forwarding path of, 116-120
root cause analysis, 83
self-assessment, 77
switch interface speed and duplex, 91-92
switch interface speeds, 92-94
layer 1 leased lines, 363-368
building WAN links, 367-368
CSU/DSU, 367
physical components, 363-365
T-carrier system, 365-367
troubleshooting, 379
layer 2 leased lines, 368-370, 380
layer 3 leased lines, 383-385
LCP (Link Control Protocol), 374-376
Learning state (STP), 36
leased line WANs
HDLC (High-level Data Link Control)
building WAN links, 367-368
CSU/DSU, 367
explained, 362

HDLC configuration, 370-372
layer 1 leased lines, 363-368
layer 2 leased lines, 368-370
leased line components, 363-365
T-carrier system, 365-366
PPP (Point-to-Point Protocol)
authentication, 375-376
CHAP (Challenge Handshake Authentication Protocol), 377-383
configuring, 376-377
explained, 373
framing, 374
LCP (Link Control Protocol), 374-375
NCP (Network Control Protocols), 374
self-assessment, 359-361
troubleshooting, 378-379
keepalive failure, 381
layer 1 problems, 379
layer 2 problems, 380
layer 3 problems, 383-385
PAP/CHAP authentication failure, 382-383
leased lines, 447-448
license boot module c2900 technology-package command, 622
license boot module command, 618
license install command, 622
licensing (IOS), 605
IOS packaging, 607
images per feature set combination, 608
images per model/series, 607
universal images, 609
IOS software activation, 609-610
Cisco License Manager (CLM), 611
manual activation, 612-617
right-to-use licenses, 618-620
license status, showing, 614-615
permanent technology package license, adding, 616-617
self-assessment, 605-606
line status, 89
Link Control Protocol (LCP), 374
link-local addresses, 474
link-state advertisements. *See* LSAs
link-state databases (LSDB), 238-239
link-state routing protocols, OSPFv2, 679-680
Link-State Update (LSU), 237, 273
link types, 662
Listening state (STP), 35
LMI (Local Management Interface), 392-397, 415-416
load balancing
EIGRPv4 (Enhanced Interior Gateway Routing Protocol version 4), 311-313
EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 537
HSRP (Hot Standby Router Protocol), 192
OSPFv2 (Open Shortest Path First version 2), 262
OSPFv3 (Open Shortest Path First version 3), 508
PSVT+ (Per-VLAN Spanning Tree Plus), 48
local DLCI (data link connection identifiers), 398-399
local loop, 455
Local Management Interface (LMI), 392-397, 415-416
logging with Syslog
configuring, 568-569
explained, 566

Syslog server, 569
system message format, 567
system message severity levels, 567-568
verifying, 568-569
logging buffered command, 568
logging console command, 568
Long-Term Evolution (LTE), 460
loops, avoiding, 284
LSAs (link-state advertisements)
exchanging with neighbors, 237
explained, 244
in multi-area design, 247-248
network LSAs, 245-247
OSPFv3 LSAs
troubleshooting, 519-520
verifying, 517-519
router LSAs, 245
verifying, 258
LSDB (link-state databases), 238-239
LSUs (Link-State Update), 237, 273
LTE (Long-Term Evolution), 460

M

MAC address tables
STP (Spanning Tree Protocol), 23-24
viewing, 17-19
maintaining OSPFv2 neighbors, 238-239
Management Information Base (MIB), 562-563
manual software activation, 612-613
adding permanent technology package license, 616-617
showing current license status, 614-615
mapping addresses, Frame Relay, 416-419
Inverse ARP, 419-420
static mapping, 420-421
troubleshooting, 440
math-related skills, 633-634
Max Age timers (STP), 34-35
maximum-paths command, 262-264, 294, 311-313, 319, 508, 533, 537, 548
memory (Flash), upgrading IOS software images into, 581-584
message logging. *See* Syslog
metric calculation (EIGRP), 280-284
metrics
EIGRPv4 (Enhanced Interior Gateway Routing Protocol version 4), 310-314
OSPFv2 (Open Shortest Path First version 2)
interface costs, 260-261
reference bandwidth, 261
MetroE (Metropolitan Ethernet), 450
MIB (Management Information Base), 562-563
microseconds, 282
mismatched IPv4 settings, 158-159
mismatched masks, 160-161
mismatched MTU settings, 346-347
mismatched OSPF network types, 345-346
mismatched subnet numbers, 441
mobile phone 3G/4G access, 459-460
MPLS (Multiprotocol Label Switching), 451
mst parameter (spanning-tree mode command), 663
MTU settings, troubleshooting, 346-347

multi-area design, LSAs (link-state advertisements) in, 247-248
multi-area OSPFv2 configuration, 252-259
multi-area OSPFv3 configuration, 503-506
multiple frame transmission, 23-24
multipoint subinterfaces, Frame Relay configuration, 426-429
Multiprotocol Interconnect over Frame Relay, 398
Multiprotocol Label Switching (MPLS), 451

N

name resolution (DNS), 147
NBMA (nonbroadcast multiaccess) networks, 392-394
NDP (Neighbor Discovery Protocol), 475
neighbors
EIGRPv4 neighbors, 278-279
displaying status of, 300-301
troubleshooting, 335-339
verification checks, 337-338
EIGRPv6 neighbors, 541-543
OSPFv2 neighbors
adjacent neighbors, 240
area mismatches, 341-342
duplicate router IDs, 342-343
exchanging LSAs (link-state advertisement) with neighbors, 237
forming neighbor relationships, 236-237
fully adjacent neighbors, 240
Hello/dead timer mismatches, 343-345
LSDB (link-state databases), 238-239
maintaining, 238-239
states, 240
troubleshooting, 335-336, 339-345
OSPFv3 (Open Shortest Path First version 3) neighbors
troubleshooting, 514-517
verifying, 513-514
NetFlow
configuring, 572
explained, 570-571
NetFlow collector, 575
network flows, 571-572
verifying, 573-574
netsh interface ipv6 show neighbors command, 496
network area command, 252, 502
network command, 264, 294-296, 319, 326, 526, 533, 681
network diagrams, confirming via CDP (LAN switching), 86-88, 104-105
network flows, 571-572
network LSAs (link-state advertisements), 245-247
network management
configuration files, 595-597
copying, 597-599
erasing, 597-599
running-config, 596
setup mode, 599
startup-config, 596
IOS software
boot sequence, 584-591
upgrading images into Flash memory, 581-584

NetFlow
configuring, 572
explained, 570-571
NetFlow collector, 575
network flows, 571-572
verifying, 573-574
password recovery
example, 592-595
explained, 591-592
self-assessment, 557-559
SNMP (Simple Network Management Protocol)
community strings, 563
explained, 560-562
MIB (Management Information Base), 562-563
SNMP version 2c, 563-565
SNMP version 3, 565
traps, 561
Syslog (System Message Logging)
configuring, 568-569
explained, 566
Syslog server, 569
system message format, 567
system message severity levels, 567-568
verifying, 568-569
Network Management Station (NMS), 561
network types (OSPF), troubleshooting, 345-346
NMS (Network Management Station), 561
no auto-summary command, 317-319
no cdp enable command, 88
no cdp run command, 88
no frame-relay inverse-arp command, 443
no frame-relay lmi-type command, 433, 443
no ip domain-lookup command, 162
no ip split-horizon eigrp asn command, 686
no ipv6 eigrp 1 command, 541
no keepalive command, 426
no logging buffered command, 568
no logging console command, 568
no passive-interface command, 264, 319
no shutdown command, 72, 95-96, 109, 370, 387, 548
no shutdown vlan command, 100
noAuthNoPriv security level, 565
nonbroadcast multiaccess (NBMA) networks, 392-394
notconnect state (LAN switches), 90
numeric reference table
binary-to-hexadecimal conversion, 652
decimal-to-binary conversion, 649-651
hexadecimal-to-binary conversion, 652

O

Open Shortest Path First. *See* OSPFv2; OSPFv3
operating systems
selection process, 586-588
three router operating systems, 585
OSPF routes, 672
OSPFv2 (Open Shortest Path First version 2), 231
AD (administrative distance), 250-251

areas
design advantages, 243
design rules, 241-242
design terminology, 242
explained, 240-241
intra-area topology, 245-247
multi-area design, 247-248
reducing SPF calculation time with, 242-243
single-area OSPF, 240
basic configuration, 251-252
compared to OSPFv3, 509-510
compared to other routing protocols, 271, 277
configuring, 680-683
default routes, 679-680
DRs (designated routers), 239-240
explained, 234-235
Frame Relay configuration, 429
load balancing, 262
LSAs (link-state advertisements)
exchanging with neighbors, 237
explained, 244
in multi-area design, 247-248
network LSAs, 245-247
router LSAs, 245
verifying, 258
LSDB (link-state databases), 238-239
metrics
interface cost, 260-261
reference bandwidth, 261
multi-area configuration, 252-256
neighbors
adjacent neighbors, 240
area mismatches, 341-342
duplicate router IDs, 342-343
exchanging LSAs with neighbors, 237
forming neighbor relationships, 236-237
fully adjacent neighbors, 240
Hello/dead timer mismatches, 343-345
maintaining, 238-239
states, 240
troubleshooting, 339-345
RID (router ID), 235
self-assessment, 231-233
single-area configuration, 254-255
SPF route calculation
calculating best routes, 248-250
reducing calculation time with areas, 242-243
troubleshooting
area mismatches, 341-342
duplicate router IDs, 342-343
Hello/dead timer mismatches, 343-345
interfaces, 325-326, 332-335
mismatched MTU settings, 346-347
mismatched network types, 345-346
neighbors, 335-336, 339-345
network types, 345-346
overview, 324-325
self-assessment, 323
verifying configuration, 256-259
areas, 256-257
DRs (dedicated routers) and BDRs (backup DRs), 257
LSAs (link-state advertisements), 258
OSPF routes, 259

OSPFv3 (Open Shortest Path First version 3), 499
basic configuration, 502
compared to OSPFv2, 509-510
default routes, 508-509
interfaces
cost, 507-508
troubleshooting, 512-513
verifying, 511
IPv6 routes, troubleshooting, 523-524
load balancing, 508
LSAs (link-state advertisements)
troubleshooting, 519-520
verifying, 517-519
metrics, verifying, 520-522
multi-area configuration, 503-506
neighbors
troubleshooting, 514-517
verifying, 513-514
self-assessment, 499-501
single-area configuration, 504-505
overlapping subnets
configuring, 177-178
with VLSM, 176
without VLSM, 174-176

P

packaging (IOS)
explained, 607
images per feature set combination, 608
images per model/series, 607
universal images, 609
packet filtering with ACLs (access control lists), 178-180
PAP/CHAP authentication failure, 382-383
partial-mesh networks, 395
partial update messages, 276
passive-interface command, 264, 298, 319, 326-327, 331, 349, 513
passive-interface default command, 264, 319
password recovery
example, 592-595
explained, 591-592
periodic update messages, 273
permanent keyword (ip route command), 671
permanent virtual circuits (PVC), 393, 433-440
Per-VLAN Spanning Tree Plus (PVST+), 47-48
physical subinterfaces, EIGRP on, 684-686
PID (product ID), 612
ping command, 480-481, 496
extended ping
LAN neighbors, testing, 145
reverse routes, testing, 142-144
IPv4 testing
explained, 137-139
with hostnames and IP addresses, 146-147
LAN neighbors, 144-145
longer routes, 139-142
reverse routes, 142-144
sample output, 138
WAN neighbors, 145-146
troubleshooting in IPv4
neighboring devices over Ethernet, 676
over serial links with ACLs (access control lists), 673-676
troubleshooting in IPv6, 484-487
ping6 command, 480, 496

pinouts (cabling) for LAN switches, 90
point of presence (PoP), 455
point-to-multipoint subinterfaces, EIGRP on, 684-686
point-to-point edge ports, 663
point-to-point links, 662
point-to-point ports, 662
Point-to-Point Protocol. *See* PPP
point-to-point subinterfaces
configuring, 421-424
EIGRP on, 684-686
point-to-point WANs
HDLC (High-level Data Link Control)
building WAN links, 367-368
CSU/DSU, 367
explained, 362
HDLC configuration, 370-372
layer 1 leased lines, 363-368
layer 2 leased lines, 368-370
leased line components, 363-365
T-carrier system, 365-366
PPP (Point-to-Point Protocol)
authentication, 375-376
CHAP (Challenge Handshake Authentication Protocol), 377-383
configuring, 376-377
explained, 373
framing, 374
LCP (Link Control Protocol), 374-375
NCP (Network Control Protocols), 374
troubleshooting, 378-379
keepalive failure, 381
layer 1 problems, 379
layer 2 problems, 380
layer 3 problems, 383-385
PAP/CHAP authentication failure, 382-383
PoP (point of presence), 455
PortFast, 37-38, 56-58
port roles, configuring, 666-667
port states, 667
port types, 662-663, 668-669
ports
alternate (root) ports, 659-660
DPs (designated ports)
choosing, 31-32
determining, 66
explained, 26
RSTP (Rapid Spanning Tree Protocol), 661-662
strategies for DP exam questions, 67-68
point-to-point edge ports, 663
point-to-point ports, 662
port roles, configuring, 666-667
port costs, 32-33
port states, 660-661, 667
port types, 662-663, 668-669
RPs (root ports)
choosing, 29-31
determining, 63-64
explained, 26
RSTP (Rapid Spanning Tree Protocol), 659-660
STP tiebreakers when choosing RP, 64-65
strategies for RP exam questions, 65-66
security
configuring on Cisco Catalyst switches, 95
LAN switching, 94-98, 107-109

shared ports, 663
STP (Spanning Tree Protocol) port cost, 53-55
powers of 2 numeric reference table, 653
PPP (Point-to-Point Protocol)
LCP authentication, 376
leased-line WANs
authentication, 375-376
CHAP (Challenge Handshake Authentication Protocol), 377-378, 382-383
configuring, 376-377
explained, 373
framing, 374
LCP (Link Control Protocol), 374-375
NCP (Network Control Protocols), 374
ppp authentication command, 387
PPPoE (PPP over Ethernet)
configuring, 461-462
explained, 460-461
pppoe-client command, 462
practice exams, 635
additional practice exams, 639-640
CCNA practice exams, 636-637
exam-taking tips, 638-639
ICND2 practice exams, 635-636
Question Review, 640-642
predicting normal IPv4 routing behavior
data link headers, 136-137
host IPv4 routing logic, 132-133
IP routing from host to host, 135
IP routing logic on single router, 134-135
sample ARP process, 137
pre-exam suggestions (Cisco Certification Exam), 631-632
PRI (Primary Rate Interface), 456
Primary Rate Interface (PRI), 456
priority of switches, configuring, 55-56
private WANs (wide area networks)
explained, 447
Frame Relay, 449
leased lines, 447-448
problem isolation
IPv4 routing problems
ping command, 137-147
traceroute command, 147-153
LAN switching, 82-83
product ID (PID), 612
protocol status, 89
protocols. *See* specific protocols
public WANs (wide area networks), 453
3G/4G mobile phone access, 459-460
Cable Internet, 457-458
dial access with modems and ISDN, 454-456
DSL (digital subscriber line), 456-457
Internet Access Links, 453
PPPoE (PPP over Ethernet)
configuring, 461-462
explained, 460-461
PVC (permanent virtual circuits)
Frame Relay, 393
status codes, 438-439
subinterface status, 439
troubleshooting in Frame Relay, 433-440
pvst parameter (spanning-tree mode command), 664
PVST+ (Per-VLAN Spanning Tree Plus), 47-48

Q

query/reply process (EIGRP), 287
Question Review, 640-642
question types (Cisco Certification Exam), 629-630

R

Rapid Spanning Tree Protocol. *See* RSTP (Rapid Tree Spanning Protocol)
rapid-pvst parameter (spanning-tree mode command), 665-666
RD (reported distance), 284-285
read-only (RO) community strings, 563
read-write (RW) community strings, 563
recovery
  passwords
    example, 592-595
    explained, 591-592
  recovery if IOS does not load, 588-589
redundancy. *See* FHRP (First Hop Redundancy Protocol)
reference bandwidth, 260-261
Relay (DHCP), troubleshooting, 166-167
releases, 607
Reliable Transport Protocol (RTP), 279
reload command, 598, 602
remote-access VPNs (virtual private networks), 208
replies (ARP), forwarding path of, 116-120
reported distance (RD), 284-285
requests
  ARP requests (broadcast), forwarding path of, 113-116
  ICMP Echo Requests, 151
resetting passwords
  example, 592-595
  explained, 591-592
reverse routes, 151
RID (router ID), 235
right-to-use licenses, 618-620
RIP steady-state operations, 273-274
RIP-2, 271, 277
RO (read-only) community strings, 563
ROAS (Router on a Stick), 163-166
ROMMON mode, 585, 592-593
root cause analysis, 83
root cost, 26
root ports (RPs)
  choosing, 29-31
  determining, 63-64
  explained, 26
  RSTP (Rapid Spanning Tree Protocol), 659-660
  STP tiebreakers when choosing RP, 64-65
  strategies for RP exam questions, 65-66
root switches
  determining, 62-63
  electing via STP, 27-29
route calculation (EIGRPv4)
  bandwidth issues, 283-284
  example, 281-283
  FD (feasible distance), 284-285
  metric calculation, 280-281
  RD (reported distance), 284-285
route poisoning, 275-276

route redistribution, 250
router eigrp command, 294-295, 319, 332, 533
router ID (RID), 235
router-id command, 235, 252, 264, 502, 504, 526
router LSAs (link-state advertisements), 245
Router on a Stick (ROAS), 163-166
router ospf command, 252, 264, 332, 502, 526
routers
active virtual gateway (AVG), 193
clock speed, 368-370
FHRP (First Hop Redundancy Protocol). *See* FHRP
for VPNs (virtual private networks), 209
routing. *See* IPv4 routing; IPv6 routing
routing protocols, OSPFv2, 679-680
routing table (IPv4), displaying, 301-302
RPs (root ports)
choosing, 29-31
determining, 63-64
explained, 26
STP tiebreakers when choosing RP, 64-65
strategies for RP exam questions, 65-66
RSTP (Rapid Spanning Tree Protocol), 36-39, 658-659
alternate (root) ports, 659-660
backup (designated) ports, 661-662
capabilities, 657-658
configuring
identifying STP mode on Catalyst swtiches, 663-666
port roles, 666-667
port states, 660-661, 667
port types, 662-663, 668-669
shared ports, 663
RTP (Reliable Transport Protocol), 279
running-config, 596
RW (read-write) community strings, 563
RxBoot operating system, 585

S

scaling
OSPFv2 with areas
design advantages, 243
design rules, 241-242
design terminology, 242
explained, 240-241
intra-area topology, 245-247
multi-area design, 247-248
reducing SPF calculation time with, 242-243
single-area OSPF, 240
VPNs (virtual private networks), 209
Secure Shell (SSH), 137
Secure Socket Layer (SSL) VPNs, 211-212
security
port security, 94-98, 107-109
VPNs (virtual private networks), 207
securityk9, 610
self-assessments
EIGRPv4 (Enhanced Interior Gateway Routing Protocol version 4), 267-268, 291-293
EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 529-531
FHRP (First Hop Redundancy Protocol), 183-185

Frame Relay, 389-391, 409-411
IOS file management, 579-581
IOS licensing, 605-606
IPv4 routing, 131, 157
IPv6 troubleshooting, 471
LAN switching, 77
leased-line WANs, 359-361
network management, 557-559
OSPFv2 (Open Shortest Path First version 2), 231-233
OSPFv3 (Open Shortest Path First version 3), 499-501
routing protocol troubleshooting, 323
STP (Spanning Tree Protocol), 13-15, 43-45
VPNs (virtual private networks), 205-206
WAN (wide area network) technologies, 445-446

self ping, 674-675
serial cables, 364
serial links, troubleshooting, 378-379
ACLs (access control lists), 673-676
keepalive failure, 381
layer 1 problems, 379
layer 2 problems, 380
layer 3 problems, 383-385
PAP/CHAP authentication failure, 382-383
serial number (SN), 612
servers, Syslog, 569
service providers, 363
session keys, 210
setup command, 599, 602
setup mode, 599
severity levels (Syslog), 567-568
shared keys, 210
shared ports, 663
shared session keys, 210
show access-lists command, 180
show arp command, 163
show cdp command, 87-88
show cdp entry command, 87, 104
show cdp neighbors command, 87, 104
show cdp neighbors detail command, 87
show command, 109, 534, 663
show controllers command, 371
show controllers serial command, 370, 387
show etherchannel command, 58, 75
show etherchannel summary command, 70
show flash command, 583, 602
show frame-relay lmi command, 433, 443
show frame-relay map command, 419-420, 426-428, 437, 440, 443
show frame-relay pvc command, 419, 425, 435, 438, 443
show glbp brief command, 198-200
show glbp command, 200-201
show interface switchport command, 99, 102
show interfaces command, 89-93, 106, 260, 281, 313, 349, 377, 387, 441-443
show interfaces description command, 89, 169, 349, 372
show interfaces status command, 19-20, 89, 91-92, 105
show interfaces trunk command, 20-21, 100
show interfaces tunnel command, 219
show ip access-lists command, 180
show ip cache flow command, 573
show ip eigrp interfaces command, 297-298, 320, 326-330, 332-333, 349

show ip eigrp interfaces detail command, 298, 320
show ip eigrp neighbors command, 300, 320, 337, 349
show ip eigrp topology all-links command, 308
show ip eigrp topology command, 281, 303-310, 320
show ip flow export command, 574
show ip flow interface command, 574
show ip interface brief command, 218, 335, 372, 387, 441-443
show ip interfaces command, 179-180
show ip ospf command, 265, 349, 526
show ip ospf database command, 244, 258, 265
show ip ospf interface brief command, 256-257, 265, 326, 332-333, 349, 526
show ip ospf interface command, 256-257, 265, 344, 349, 526, 683
show ip ospf neighbor command, 235-236, 239-240, 257, 265, 339-340, 349
show ip protocols command, 256, 265, 297-301, 320, 326, 329-334, 338, 349, 526, 682
show ip route command, 170-172, 220, 251, 265, 302, 315, 320, 537, 670, 673
command output, 172-173
finding best route with, 172
overlapping routes, 170-171
show ip route eigrp command, 301-302, 330, 349
show ip route ospf command, 171, 265, 349
show ip route | section command, 320
show ip route static command, 670
show ip route subnet command, 673
show ipv6 eigrp interfaces command, 540, 548
show ipv6 eigrp interfaces detail command, 548
show ipv6 eigrp neighbors command, 541-542, 548-549
show ipv6 eigrp topology command, 543, 549
show ipv6 eigrp topology | section command, 549
show ipv6 interface command, 493, 496
show ipv6 neighbors command, 483, 496
show ipv6 ospf command, 495-496, 522
show ipv6 ospf database command, 496, 527
show ipv6 ospf interface brief command, 496, 511-512, 522
show ipv6 ospf interface command, 511-512, 517
show ipv6 ospf neighbor command, 496, 513, 516, 520, 527
show ipv6 protocols command, 496, 511, 540, 542, 548
show ipv6 route command, 495, 527, 537, 549
show ipv6 route eigrp command, 549
show ipv6 route ospf command, 521, 527
show ipv6 route | section command, 549
show ipv6 routers command, 496
show license command, 615, 619
show license feature command, 615, 622
show license udi command, 612, 622
show logging command, 568-569
show mac address-table command, 19, 99, 119

show mac address-table dynamic command, 18, 99, 119
show port-security command, 107-108
show port-security interface command, 95-97
show running-config command, 57, 180, 297, 371, 511, 596, 602
show spanning-tree bridge command, 56, 75
show spanning-tree command, 50-52, 60-63, 66-67, 75, 113, 668
show spanning-tree interface command, 75
show spanning-tree root command, 52, 56, 62-63, 75
show spanning-tree vlan command, 62, 75, 100, 666-667
show standby brief command, 196-197
show standby command, 197
show startup-config command, 596
show version command, 589-591, 615-617, 622
show vlan brief command, 20, 99
show vlan command, 20, 99
show vlan id command, 99
shutdown command, 72, 96, 109, 387, 548
Simple Network Management Protocol. *See* SNMP
single-area OSPF (Open Shortest Path First), 240
single-area OSPFv2 configuration, 254-255
single-area OSPFv3 configuration, 504-505
single points of failure, 186-188
site-to-site VPNs (virtual private networks), 207-208
SLAAC (stateless address autoconfiguration), 472, 476-477, 489-490
SMARTnet, 609
SN (serial number), 612
SNMP (Simple Network Management Protocol)
community strings, 563
explained, 560-562
MIB (Management Information Base), 562-563
SNMP version 2c, 563-565
SNMP version 3, 565
traps, 561
SNMPGET utility, 563
snmp-server community command, 564
snmp-server contact command, 564
snmp-server location command, 564
software activation (IOS), 609-610
Cisco License Manager (CLM), 611
manual activation
activation process, 612-615
adding permanent technology package license, 616-617
right-to-use licenses, 618-620
self-assessment, 605-606
spanning tree algorithm (STA), 25
Spanning Tree Protocol. *See* STP
spanning-tree bpduguard default command, 58
spanning-tree bpduguard disable command, 58, 74
spanning-tree bpduguard enable command, 57, 74
spanning-tree cost command, 68
spanning-tree mode command, 74, 663, 667
spanning-tree mode mst command, 47

spanning-tree mode pvst command, 47, 664
spanning-tree mode rapid-pvst command, 47, 665-666
spanning-tree portfast bpduguard default command, 74
spanning-tree portfast command, 57, 74
spanning-tree portfast default command, 58, 74
spanning-tree portfast disable command, 58, 74
spanning-tree vlan vlan-id priority value command, 55
spanning-tree vlan vlan-id priority x command, 49, 74
spanning-tree vlan vlan-id root primary command, 55
spanning-tree vlan vlan-id root secondary command, 55
spanning-tree vlan vlan-number port-priority priority command, 74
spanning-tree vlan vlan-number root secondary command, 74
spanning-tree vlan x cost command, 49, 53-54, 74
speed command, 92
SPF route calculation
calculating best routes, 248-250
reducing calculation time with areas, 242-243
split horizon, 274-275, 684-686
SSH (Secure Shell), 137
SSL (Secure Socket Layer) VPNs, 211-212
STA (spanning tree algorithm), 25
standby command, 195
startup-config, 596
stateful DHCPv6, 475, 488-489
stateless address autoconfiguration. *See* **SLAAC**
states of OSPFv2 neighbors, 240
states (port), 660-661, 667
static address mapping, 420-421
static router configuration (IPv6), 478-479
static routes, configuring, 669-671
with competing routes, 672-673
with no competing routes, 671
steady-state networks (STP), 33
steady-state operations (RIP), 273-274
STP (Spanning Tree Protocol), 13, 43. ***See also*** RSTP (Rapid Spanning Tree Protocol)
BID (bridge ID), 27
blocking state, 24-26
BPDU (bridge protocol data units), 27
BPDU Guard feature, 38
broadcast storms, 22-24
configuring, 46
BID (bridge ID), 48-49
BPDU Guard, 56-58
defaults and configuration options, 49-50
EtherChannel, 58-61
per-VLAN configuration settings, 47-48
per-VLAN costs, 49
port costs, 54
PortFast, 56-58
STP mode, 47
STP port costs, 53-55
switch priority, 54-56
system ID extension, 48-49
convergence, 25, 35
delays, 36
troubleshooting, 68

DPs (designated ports)
choosing, 31-32
determining, 66
explained, 26
strategies for DP exam questions, 67-68
EtherChannel, 37
explained, 21-22
forwarding state, 24-25
reasons for, 26
root switches, 26-29
interface state changes, 35-36
Learning state, 36
Listening state, 35
MAC table instability, 23-24
multiple frame transmission, 23-24
need for, 22-24
port costs, 32-33
PortFast, 37-38
PSVT+ (Per-VLAN Spanning Tree Plus), 47
root switches
determining, 62-63
electing, 27-29
RPs (root ports)
choosing, 29-31
determining, 63-64
explained, 26
STP tiebreakers when choosing RP, 64-65
strategies for RP exam questions, 65-66
self-assessment, 13-15, 43-45
STA (spanning tree algorithm), 25
state comparison table, 36
steady-state networks, 33
timers, 34-35
topology
influencing with configuration changes, 32-33
interface state changes, 35-36
reacting to state changes that affect STP topology, 33
simple STP tree, 24-25
switch reactions to changes with STP, 34-35
troubleshooting, 61
convergence, 68
DPs (designated ports), 66-68
EtherChannel, 68-72
root switches, 62-63
RPs (root ports), 63-66
verifying default operation, 51
verifying STP operation, 50-53
subinterfaces, 403
multipoint subinterfaces, 426-429
point-to-point subinterfaces, configuring, 421-424
subnet masks, troubleshooting, 160-161
subnets, 633-634
Frame Relay networks
fully meshed networks with one IP subnet, 413-415
hybrid Layer 3 addressing, 404-405
one subnet containing all Frame Relay DTEs, 401-402
one subnet per VC, 402-403
IPv6, 472-474
mismatched masks, troubleshooting, 160-161
mismatched subnet numbers, troubleshooting, 441

overlapping subnets
configuring, 177-178
with VLSM, 176
without VLSM, 174-176
successors (EIGRP), 285-287
feasible successors, creating/viewing, 308
finding, 305-306
superior hello (STP), 28
SVC (switched virtual circuits), 393
switch priority, configuring, 55-56
switch verification (LAN), 17
determining VLAN of frames, 19-20
verifying trunks, 20-21
viewing MAC address table, 17-19
switchport access vlan command, 99, 110, 166
switchport mode access command, 98, 166
switchport mode trunk command, 98, 164
switchport port-security command, 98
switchport port-security mac-address command, 98, 119
switchport port-security mac-address sticky command, 98
switchport port-security violation command, 94, 98
switchport trunk allowed vlan command, 100
switchport trunk mode command, 102
switchport trunk native vlan command, 164
Syslog (System Message Logging)
configuring, 568-569
explained, 566
Syslog server, 569
system message format, 567
system message severity levels, 567-568
verifying, 568-569
system ID extension, configuring, 48-49
System Message Logging. *See* Syslog

T

T-carrier system, 365-366
tables, MAC address tables, 17-19, 23
TDM (time-division multiplexing), 366
tens-of-microseconds, 282
testing IPv4 routing with ping command
with hostnames and IP addresses, 146-147
LAN neighbors, 144-145
longer routes, 139-142
reverse routes, 142-144
WAN neighbors, 145-146
time burners, 630
time-division multiplexing (TDM), 366
time management (Cisco Certification Exam), 630-631
Time To Live (TTL), 148
Time-to-Live Exceeded (TTL Exceeded), 148
timers
Dead Interval, 238
EIGRPv6, 538
Hello/dead timer mismatches, finding, 343-345
Hello Interval, 238
topology table
EIGRPv4
convergence, 308-310
feasible successor routes, 306-308

successor routes, 305-306
viewing, 303-305
EIGRPv6, 543-545
traceroute command, 147, 480-481, 496
explained, 147-150
extended traceroute, 150-151
GRE (generic routing encapsulation) tunnels, verifying, 220
isolating problems to two routers, 151-153
sample output, 148
standard traceroute, 150
troubleshooting in IPv6, 490-493
traceroute6 command, 496
traps (SNMP), 561
Triple DES (3DES), 211
troubleshooting
CHAP (Challenge Handshake Authentication Protocol), 382-383
EIGRPv4 (Enhanced Interior Gateway Routing Protocol version 4)
interfaces, 325-332
neighbors, 335-339
overview, 324-325
self-assessment, 323
EtherChannel
channel-group command options, 68-70
interface configuration settings, 70-72
Frame Relay, 430
end-to-end encapsulation, 441
Layer 1 issues on access links, 432
Layer 2 issues on access links, 432
mapping issues, 440
mismatched subnet numbers, 441
PVC (permanent virtual circuit) problems, 433-440
self-assessment, 409-411
suggested process, 430-431
IPv4 routing, 131, 157-158
ACLs (access control lists), 178-180, 673-676
DHCP Relay issues, 166-167
DNS problems, 161-162
IP address settings, 163
IP forwarding, 170-173
LAN issues, 167-169
mismatched IPv4 settings, 158-159
mismatched masks, 160-161
mismatched VLAN trunking configuration, 163-166
normal routing behavior, predicting, 132-137
with ping command, 137-147
router WAN interface status, 178
self-assessment, 131, 157
with show ip route command, 170-173
with traceroute command, 147-153
VLSM, 174-178
IPv6 routing, 483-484
DNS issues, 487
ping failures, 484-487
self-assessment, 471
SLAAC issues, 489-490
stateful DHCP, 488-489
traceroute failures, 490-493

LAN switching, 77-78
analyzing/predicting normal operation, 79-82
ARP Reply (unicast), forwarding path of, 116-120
ARP requests (broadcast), forwarding path of, 113-116
cabling pinouts, 90
control plane analysis, 81
data plane analysis, 79-81
duplex issues, 92-94
exam tips, 84
example of, 109
forwarding process overview, 16-17, 85-86
interface status codes, 88-89
isolate filtering/port security problems, 94-98, 107-109
isolation of interface problems, 88-94, 105-107
isolation of VLAN/trunking problems, 20-21, 98-102, 109-112
network diagram confirmation via CDP, 86-88, 104-105
notconnect state, 90
problem isolation, 82-83
root cause analysis, 83
self-assessment, 77
switch interface speed and duplex, 91-92
switch interface speeds, 92-94
OSPFv2 (Open Shortest Path First version 2)
area mismatches, 341-342
duplicate router IDs, 342-343
Hello/dead timer mismatches, 343-345
interfaces, 325-326, 332-335
mismatched MTU settings, 346-347
mismatched network types, 345-346
neighbors, 335-345
overview, 324-325
self-assessment, 323
OSPFv3 (Open Shortest Path First version 3)
interfaces, 512-513
IPv6 routes, 523-524
LSAs (link-state advertisements), 519-520
neighbors, 514-517
serial links, 378-379
keepalive failure, 381
layer 1 problems, 379
layer 2 problems, 380
layer 3 problems, 383-385
PAP/CHAP authentication failure, 382-383
STP (Spanning Tree Protocol), 61
convergence, 68
DPs (designated ports), 66-68
EtherChannel, 68-72
root switches, 62-63
RPs (root ports), 63-66
VLSM
overlapping subnets, 176-178
recognizing when VLSM is used, 174
trunking
mismatched VLAN trunking configuration, 163-166
verifying, 20-21, 111-112
trunking problems, isolating, 20-21, 98-102, 109-112
TTL (Time To Live), 148

TTL Exceeded (Time-to-Live Exceeded), 148
tunnel destination command, 217, 222
tunnel interfaces, 213-215
tunnel mode gre command, 222
tunnels
explained, 208
GRE (generic routing encapsulation) tunnels
configuring, 216-218
explained, 212
over unsecured network, 214-216
routing over, 213-214
tunnel interfaces, 213-215
verifying, 218-220
VPN tunnels, 207-208
tunnel source command, 217, 222
Two-way neighbor state (OSPF neighbors), 240

U

uck9, 610
UDI (unique device identifier), 612
undebug all command, 350
unequal-cost load balancing, 311
unicast IPv6 addresses, 472-474
unicasts, forwarding, 117-119
unique device identifier (UDI), 612
universal images
explained, 609
IOS software activation, 609-610
Cisco License Manager (CLM), 611
manual activation, 612-617
right-to-use licenses, 618-620
unsecured networks, GRE (generic routing encapsulation) tunnels, 214-216
update messages (EIGRP), 279-280
upgrading images into Flash memory, 581-584
username command, 387

V

variance, 311-313
variance command, 294, 311-312, 319, 533, 537, 548
VC (virtual circuits)
CIR (committed information rate), 394
explained, 393-396, 402-403
verifying
EIGRPv4 core features, 296-297
interfaces, 297-300
IPv4 routing table, 301-302
neighbor status, 300-301, 337-338
Frame Relay configurations, 424-426
GLBP (Gateway Load Balancing Protocol), 198-201
GRE (generic routing encapsulation) tunnels, 218-220
HSRP (Hot Standby Router Protocol), 195-197
IOS images, 589-591
IPv6 connectivity
from hosts, 479-480
from routers, 481-483
LAN switches
determining VLAN of frames, 19-20
verifying trunks, 20-21
viewing MAC address table, 17-19

NetFlow, 573-574
OSPFv2 (Open Shortest Path First version 2), 256-259
areas, 256-257
configuration, 682-683
DRs (dedicated routers) and BDRs (backup DRs), 257
LSAs (link-state advertisements), 258
OSPF routes, 259
OSPFv3 (Open Shortest Path First version 3)
interfaces, 511
LSAs (link-state advertisements), 517-519
metrics, 520-522
neighbors, 513-514
STP (Spanning Tree Protocol) operation, 50-53
Syslog (System Message Logging), 568-569
trunking and VLAN 3, 111-112

very small aperture terminal (VSAT), 452

virtual circuits (VC)
explained, 393-396
Layer 3 addressing, 402-403

Virtual Private LAN Service (VPLS), 450

virtual private networks. *See* VPNs

Virtual Router Redundancy Protocol (VRRP), 190

VLANs
access interface VLAN assignments, checking, 109
active VLANs, checking for, 110
broadcast forwarding, 115-116
determining VLAN of frames, 19-20
isolating VLAN and trunking problems, 20-21, 98-102, 109-112
STP (Spanning Tree Protocol) configuration
BID (bridge ID), 48-49
per-VLAN configuration settings, 47-48
per-VLAN costs, 49
system ID extension, 48-49
trunking
mismatched VLAN trunking configuration, 163-166
verifying, 111-112

VLSM, troubleshooting, 174
overlapping subnets, 176-178
recognizing when VLSM is used, 174

VPLS (Virtual Private LAN Service), 450

VPNs (virtual private networks)
ASA (Adaptive Security Appliances), 209
clients, 209
explained, 205
extranet VPNs, 208
GRE (generic routing encapsulation) tunnels
configuring, 216-218
explained, 212
over unsecured network, 214-216
routing over, 213-214
tunnel interfaces, 213-215
verifying, 218-220
intranet VPNs, 208
IPsec VPNs, 209-211
remote-access VPNs, 208
routers, 209
scalability, 209
security, 207
self-assessment, 205-206
site-to-site VPNs, 207

SSL VPNs, 211-212
tunnels, 207
VPN tunnels, 207-208
VRRP (Virtual Router Redundancy Protocol), 190, 678-679
VSAT (very small aperture terminal), 452

W-X-Y-Z

WAN interface cards (WICs), 365
WAN neighbors, testing with ping, 145-146
WANs (wide area networks), 447
Frame Relay. *See* Frame Relay
HDLC (High-level Data Link Control)
building WAN links, 367-368
CSU/DSU, 367
explained, 362
HDLC configuration, 370-372
layer 1 leased lines, 363-368
layer 2 leased lines, 368-370
leased line components, 363-365
self-assessment, 359-361
T-carrier system, 365-366
neighbors, testing with ping, 145-146
PPP (Point-to-Point Protocol), 376
authentication, 375-376
CHAP (Challenge Handshake Authentication Protocol), 377-383
configuring, 376-377
explained, 373
framing, 374
LCP (Link Control Protocol), 374-375
NCP (Network Control Protocols), 374
private WANs
Ethernet WANs, 449-451
explained, 447
Frame Relay, 449
leased lines, 447-448
MPLS (Multiprotocol Label Switching), 451
VSAT (very small aperture terminal), 452
public WANs
3G/4G mobile phone access, 459-460
Cable Internet, 457-458
dial access with modems and ISDN, 454-456
DSL (digital subscriber line), 456-457
Internet Access Links, 453
PPPoE (PPP over Ethernet), 460-462
router WAN interface status, troubleshooting, 178
self-assessment, 445-446
troubleshooting, 378-379
keepalive failure, 381
layer 1 problems, 379
layer 2 problems, 380
layer 3 problems, 383-385
PAP/CHAP authentication failure, 382-383
VPNs (virtual private networks)
ASA (Adaptive Security Appliances), 209
clients, 209
explained, 205
extranet VPNs, 208
GRE (generic routing encapsulation) tunnels, 212-220
intranet VPNs, 208

IPsec VPNs, 209-211
remote-access VPNs, 208
routers, 209
scalability, 209
security, 207
self-assessment, 205-206
site-to-site VPNs, 207
SSL VPNs, 211-212
tunnels, 207
VPN tunnels, 207-208
WICs (WAN interface cards), 365
WICs (WAN interface cards), 365
wildcard masks, configuring EIGRPv4 with, 296
wireless Internet, 460
write erase command, 599, 602