cisco

Official Cert Guide

Learn, prepare, and practice for exam success

CCNA Routing and Switching ICND2 200-105

Academic Edition

ciscopress.com

WENDELL ODOM, CCIE® No. 1624

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

CCNA Routing and Switching
ICND2 200-105

Official Cert Guide
Academic Edition

WENDELL ODOM, CCIE No. 1624

with contributing author

SCOTT HOGG, CCIE No. 5133

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

CCNA Routing and Switching ICND2 200-105 Official Cert Guide Academic Edition

Wendell Odom with contributing author Scott Hogg

Copyright© 2017 Pearson Education, Inc.

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

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

Printed in the United States of America

First Printing August 2016

Library of Congress Control Number: 2016936746

ISBN-13: 978-1-58720-598-9

ISBN-10: 1-58720-598-X

Warning and Disclaimer

This book is designed to provide information about the Cisco ICND2 200-105 exam for CCNA Routing and Switching certification. 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.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.

Editor-in-Chief: Mark Taub

Product Line Manager: Brett Bartow

Business Operation Manager, Cisco Press: Jan Cornelssen

Managing Editor: Sandra Schroeder

Development Editor: Drew Cupp

Senior Project Editor: Tonya Simpson

Copy Editor: Bill McManus

Technical Editor(s): Aubrey Adams, Elan Beer

Editorial Assistant: Vanessa Evans

Cover Designer: Chuti Prasertsith

Composition: Bronkella Publishing

Indexer: Publishing Works, Inc.

Proofreader: Paula Lowell

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

About the Author

Wendell Odom, CCIE No. 1624 (Emeritus), 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 study tools. This book is his 27th edition of some product for Pearson, and he is the author of all editions of the CCNA Routing and Switching and CCENT Cert Guides from Cisco Press. He has written books about topics from networking basics, and certification guides throughout the years for CCENT, CCNA R&S, CCNA DC, CCNP ROUTE, CCNP QoS, and CCIE R&S. He helped develop the popular Pearson Network Simulator. He maintains study tools, links to his blogs, and other resources at http://www.certskills.com.

About the Contributing Author

Scott Hogg, CCIE No. 5133, CISSP No. 4610, is the CTO for Global Technology Resources, Inc. (GTRI). Scott authored the Cisco Press book *IPv6 Security*. Scott is a Cisco Champion, founding member of the Rocky Mountain IPv6 Task Force (RMv6TF), and a member of the Infoblox IPv6 Center of Excellence (COE). Scott is a frequent presenter and writer on topics including IPv6, SDN, Cloud, and Security.

About the Technical Reviewers

Aubrey Adams is a Cisco Networking Academy instructor in Perth, Western Australia. With a background in telecommunications design, Aubrey has qualifications in electronic engineering and management; graduate diplomas in computing and education; and associated industry certifications. He has taught across a broad range of both related vocational and education training areas and university courses. Since 2007, Aubrey has technically reviewed a number of Pearson Education and Cisco Press publications, including video, simulation, and online products.

Elan Beer, CCIE No. 1837, is a senior consultant and Cisco instructor specializing in data center architecture and multiprotocol network design. For the past 27 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 the Cisco 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.

Dedications

For Kris Odom, my wonderful wife: The best part of everything we do together in life. Love you, doll.

Acknowledgments

Brett Bartow again served as associate publisher and executive editor on the book. We've worked together on probably 20+ titles now. Besides the usual wisdom and good decision making to guide the project, he was the driving force behind adding all the new apps to the DVD/web. As always, Brett has been a pleasure to work with, and an important part of deciding what the entire Official Cert Guide series direction should be.

As part of writing these books, we work in concert with Cisco. A special thanks goes out to various people on the Cisco team who work with Pearson to create Cisco Press books. In particular, Greg Cote, Joe Stralo, and Phil Vancil were a great help while we worked on these titles.

Drew Cupp did his usual wonderful job with this book as development editor. He took over the job for this book during a pretty high-stress and high-load timeframe, and delivered with excellence. Thanks Drew for jumping in and getting into the minutia while keeping the big-picture features on track. And thanks for the work on the online/DVD elements as well!

Aubrey Adams and Elan Beer both did a great job as technical editors for this book, just as they did for the ICND1 100-105 Cert Guide. This book presented a little more of a challenge, from the breadth of some of the new topics, just keeping focus with such a long pair of books in a short time frame. Many thanks to Aubrey and Elan, for the timely input, for taking the time to read and think about every new part of the book, for finding those small technical areas, and for telling me where I need to do more. Truly, it's a much better book because of the two of you.

Hank Preston of Cisco Systems, IT as a Service Architect, and co-author of the Cisco Press *CCNA Cloud CLDADM 210-455 Cert Guide*, gave me some valuable assistance when researching before writing the cloud computing chapter (27). Hank helped me refine my understanding based on his great experience with helping Cisco customers implement cloud computing. Hank did not write the chapter, but his insights definitely made the chapter much better and more realistic.

Welcome and thanks to Lisa Matthews for her work on the DVD and online tools, like the Key Topics reviews. That work included many new math-related apps in the ICND1 book, but also many new features that sit on the DVD and on this book's website as review tools. Thanks for the hard work, Lisa!

I love the magic wand that is production. Presto, Word docs with gobs of queries and comments feed into the machine, and out pops these beautiful books. Thanks to Sandra Schroeder, Tonya Simpson, and all the production team for making the magic happen. From fixing all my grammar, crummy word choices, and passive-voice sentences to pulling the design and layout together, they do it all; thanks for putting it all together and making it look easy. And Tonya, once again getting the "opportunity" to manage two books with many elements at the same timeline. Once again, the juggling act continues, and once again, it is done well and beautifully. Thanks for managing the whole production process again.

The figures in the book continue to be an important part of the book, by design, with a great deal of attention paid to choosing how to use figures to communicate ideas. Mike Tanamachi, illustrator and mind reader, did his usual great job creating the finished figure files once again. Thanks for the usual fine work, Mike!

I could not have made the timeline for this book without Chris Burns of Certskills Professional. Chris owns the mind map process now, owns big parts of the lab development process for the associated labs added to my blogs, does various tasks related to specific chapters, and then catches anything I need to toss over my shoulder so I can focus on the books. Chris, you are the man!

Sean Wilkins played the largest role he's played so far with one of my books. A long-time co-collaborator with Pearson's CCNA Simulator, Sean did a lot of technology work behind the scenes. No way the books are out on time without Sean's efforts; thanks for the great job, Sean!

A special thanks to you readers who submit suggestions and point out possible errors, and especially to those of you who post online at the Cisco Learning Network. Without question, past comments I have received directly and "overheard" by participating at CLN have made this edition a better book.

Thanks to my wonderful wife, Kris, who helps make this sometimes challenging work lifestyle a breeze. I love walking this journey with you, doll. Thanks to my daughter Hannah. And thanks to Jesus Christ, Lord of everything in my life.

Contents at a Glance

Introduction xxxiii

Your Study Plan 2

Part I Ethernet LANs 11

Chapter 1 Implementing Ethernet Virtual LANs 12

Chapter 2 Spanning Tree Protocol Concepts 38

Chapter 3 Spanning Tree Protocol Implementation 64

Chapter 4 LAN Troubleshooting 92

Chapter 5 VLAN Trunking Protocol 114

Chapter 6 Miscellaneous LAN Topics 136

Part I Review 156

Part II IPv4 Routing Protocols 161

Chapter 7 Understanding OSPF Concepts 162

Chapter 8 Implementing OSPF for IPv4 184

Chapter 9 Understanding EIGRP Concepts 214

Chapter 10 Implementing EIGRP for IPv4 234

Chapter 11 Troubleshooting IPv4 Routing Protocols 260

Chapter 12 Implementing External BGP 286

Part II Review 310

Part III Wide-Area Networks 313

Chapter 13 Implementing Point-to-Point WANs 314

Chapter 14 Private WANs with Ethernet and MPLS 346

Chapter 15 Private WANs with Internet VPN 368

Part III Review 412

Part IV IPv4 Services: ACLs and QoS 415

Chapter 16 Basic IPv4 Access Control Lists 416

Chapter 17 Advanced IPv4 Access Control Lists 436

Chapter 18 Quality of Service (QoS) 464

Part IV Review 490

Part V IPv4 Routing and Troubleshooting 493

Chapter 19 IPv4 Routing in the LAN 494

Chapter 20 Implementing HSRP for First-Hop Routing 516

Chapter 21 Troubleshooting IPv4 Routing 536

Part V Review 556

Part VI IPv6 561

Chapter 22 IPv6 Routing Operation and Troubleshooting 562

Chapter 23 Implementing OSPF for IPv6 584

Chapter 24 Implementing EIGRP for IPv6 612

Chapter 25 IPv6 Access Control Lists 632

Part VI Review 656

Part VII Miscellaneous 659

Chapter 26 Network Management 660

Chapter 27 Cloud Computing 696

Chapter 28 SDN and Network Programmability 724

Part VII Review 744

Part VIII Final Prep 747

Chapter 29 Final Review 748

Part IX Appendixes 763

Appendix A Numeric Reference Tables 764

Appendix B CCNA ICND2 200-105 Exam Updates 770

Glossary 780

Index 816

DVD Appendixes

Appendix C Answers to the Review Questions

Appendix D Practice for Chapter 16: Basic IPv4 Access Control Lists

Appendix E Mind Map Solutions

Appendix F Study Planner

Appendix G Learning IPv4 Routes with RIPv2

Appendix H Understanding Frame Relay Concepts

Appendix I Implementing Frame Relay

Appendix J IPv4 Troubleshooting Tools

Appendix K Topics from Previous Editions

Appendix L Exam Topic Cross Reference

Contents

Introduction xxxiii

Your Study Plan 2

A Brief Perspective on Cisco Certification Exams 2

Five Study Plan Steps 3

Step 1: Think in Terms of Parts and Chapters 3

Step 2: Build Your Study Habits Around the Chapter 4

Step 3: Use Book Parts for Major Milestones 4

Step 4: Use the Final Review Chapter to Refine Skills and Uncover Weaknesses 5

Step 5: Set Goals and Track Your Progress 6

Things to Do Before Starting the First Chapter 7

Find Review Activities on the Web and DVD 7

Should I Plan to Use the Two-Exam Path or One-Exam Path? 7

Study Options for Those Taking the 200-125 CCNA Exam 8

Other Small Tasks Before Getting Started 9

Getting Started: Now 9

Part I Ethernet LANs 11

Chapter 1 Implementing Ethernet Virtual LANs 12

Foundation Topics 13

Virtual LAN Concepts 13

Creating Multiswitch VLANs Using Trunking 14

VLAN Tagging Concepts 15

The 802.1Q and ISL VLAN Trunking Protocols 16

Forwarding Data Between VLANs 16

Routing Packets Between VLANs with a Router 17

Routing Packets with a Layer 3 Switch 19

VLAN and VLAN Trunking Configuration and Verification 19

Creating VLANs and Assigning Access VLANs to an Interface 20

VLAN Configuration Example 1: Full VLAN Configuration 20

VLAN Configuration Example 2: Shorter VLAN Configuration 23

VLAN Trunking Protocol 24

VLAN Trunking Configuration 24

Implementing Interfaces Connected to Phones 28

Data and Voice VLAN Concepts 29

Data and Voice VLAN Configuration and Verification 30

Summary: IP Telephony Ports on Switches 32

Chapter Summary 33

Review Questions 33

Chapter Review 34

Chapter 2 Spanning Tree Protocol Concepts 38

Foundation Topics 39
Spanning Tree Protocol (IEEE 802.1D) 39
The Need for Spanning Tree 39
What IEEE 802.1D Spanning Tree Does 41
How Spanning Tree Works 42
The STP Bridge ID and Hello BPDU 43
Electing the Root Switch 44
Choosing Each Switch's Root Port 45
Choosing the Designated Port on Each LAN Segment 47
Influencing and Changing the STP Topology 48
Making Configuration Changes to Influence the STP Topology 48
Reacting to State Changes That Affect the STP Topology 49
How Switches React to Changes with STP 49
Changing Interface States with STP 50
Rapid STP (IEEE 802.1w) Concepts 51
Comparing STP and RSTP 52
RSTP and the Alternate (Root) Port Role 53
RSTP States and Processes 54
RSTP and the Backup (Designated) Port Role 55
RSTP Port Types 56
Optional STP Features 56
EtherChannel 57
PortFast 57
BPDU Guard 58
Chapter Summary 59
Review Questions 60
Chapter Review 61

Chapter 3 Spanning Tree Protocol Implementation 64

Foundation Topics 65
Implementing STP 65
Setting the STP Mode 65
Connecting STP Concepts to STP Configuration Options 66
Per-VLAN Configuration Settings 66
The Bridge ID and System ID Extension 67
Per-VLAN Port Costs 68
STP Configuration Option Summary 68
Verifying STP Operation 68
Configuring STP Port Costs 71
Configuring Priority to Influence the Root Election 72
Implementing Optional STP Features 74
Configuring PortFast and BPDU Guard 74

Configuring EtherChannel 76
Configuring a Manual EtherChannel 77
Configuring Dynamic EtherChannels 79
Implementing RSTP 80
Identifying the STP Mode on a Catalyst Switch 80
RSTP Port Roles 83
RSTP Port States 84
RSTP Port Types 84
Chapter Summary 86
Review Questions 86
Chapter Review 88

Chapter 4 LAN Troubleshooting 92

Foundation Topics 93
Troubleshooting STP 93
Determining the Root Switch 93
Determining the Root Port on Nonroot Switches 94
STP Tiebreakers When Choosing the Root Port 95
Suggestions for Attacking Root Port Problems on the Exam 96
Determining the Designated Port on Each LAN Segment 96
Suggestions for Attacking Designated Port Problems on the Exam 97
STP Convergence 98
Troubleshooting Layer 2 EtherChannel 98
Incorrect Options on the channel-group Command 98
Configuration Checks Before Adding Interfaces to EtherChannels 100
Analyzing the Switch Data Plane Forwarding 101
Predicting STP Impact on MAC Tables 102
Predicting EtherChannel Impact on MAC Tables 103
Choosing the VLAN of Incoming Frames 104
Troubleshooting VLANs and VLAN Trunks 105
Access VLAN Configuration Incorrect 105
Access VLANs Undefined or Disabled 106
Mismatched Trunking Operational States 107
Mismatched Supported VLAN List on Trunks 108
Mismatched Native VLAN on a Trunk 110
Chapter Summary 111
Chapter Review 111

Chapter 5 VLAN Trunking Protocol 114

Foundation Topics 115
VLAN Trunking Protocol (VTP) Concepts 115
Basic VTP Operation 115
Synchronizing the VTP Database 116
Requirements for VTP to Work Between Two Switches 118

VTP Version 1 Versus Version 2 119
VTP Pruning 119
Summary of VTP Features 120
VTP Configuration and Verification 121
Using VTP: Configuring Servers and Clients 121
Verifying Switches Synchronized Databases 123
Storing the VTP and Related Configuration 125
Avoiding Using VTP 126
VTP Troubleshooting 127
Determining Why VTP Is Not Synchronizing 127
Common Rejections When Configuring VTP 128
Problems When Adding Switches to a Network 128
Chapter Summary 131
Review Questions 131
Chapter Review 132

Chapter 6 Miscellaneous LAN Topics 136

Foundation Topics 137
Securing Access with IEEE 802.1x 137
AAA Authentication 139
AAA Login Process 139
TACACS+ and RADIUS Protocols 139
AAA Configuration Examples 140
DHCP Snooping 142
DHCP Snooping Basics 142
An Example DHCP-based Attack 143
How DHCP Snooping Works 144
Summarizing DHCP Snooping Features 145
Switch Stacking and Chassis Aggregation 146
Traditional Access Switching Without Stacking 146
Switch Stacking of Access Layer Switches 146
Switch Stack Operation as a Single Logical Switch 148
Cisco FlexStack and FlexStack-Plus 149
Chassis Aggregation 149
High Availability with a Distribution/Core Switch 149
Improving Design and Availability with Chassis Aggregation 150
Chapter Summary 152
Review Questions 152
Chapter Review 153

Part I Review 156

Part II IPv4 Routing Protocols 161

Chapter 7 Understanding OSPF Concepts 162

Foundation Topics 163
Comparing Dynamic Routing Protocol Features 163
Routing Protocol Functions 163
Interior and Exterior Routing Protocols 164
Comparing IGPs 165
IGP Routing Protocol Algorithms 165
Metrics 166
Other IGP Comparisons 167
Administrative Distance 167
OSPF Concepts and Operation 168
OSPF Overview 169
Topology Information and LSAs 169
Applying Dijkstra SPF Math to Find the Best Routes 170
Becoming OSPF Neighbors 170
The Basics of OSPF Neighbors 170
Meeting Neighbors and Learning Their Router ID 171
Exchanging the LSDB Between Neighbors 172
Fully Exchanging LSAs with Neighbors 173
Maintaining Neighbors and the LSDB 174
Using Designated Routers on Ethernet Links 174
Calculating the Best Routes with SPF 176
OSPF Area Design 177
OSPF Areas 178
How Areas Reduce SPF Calculation Time 179
OSPF Area Design Advantages 180
Chapter Summary 181
Review Questions 182
Chapter Review 183

Chapter 8 Implementing OSPF for IPv4 184

Foundation Topics 185
Implementing Single-Area OSPFv2 185
OSPF Single-Area Configuration 186
Matching with the OSPF network Command 187
Verifying OSPFv2 Single Area 188
Configuring the OSPF Router ID 191
OSPF Passive Interfaces 192
Implementing Multiarea OSPFv2 194
Single-Area Configurations 195
Multiarea Configuration 196

Verifying the Multiarea Configuration 197
Verifying the Correct Areas on Each Interface on an ABR 198
Verifying Which Router Is DR and BDR 198
Verifying Interarea OSPF Routes 199
Additional OSPF Features 200
OSPF Default Routes 200
OSPF Metrics (Cost) 202
Setting the Cost Based on Interface Bandwidth 202
The Need for a Higher Reference Bandwidth 204
OSPF Load Balancing 204
OSPFv2 Interface Configuration 205
OSPFv2 Interface Configuration Example 205
Verifying OSPFv2 Interface Configuration 206
Chapter Summary 208
Review Questions 208
Chapter Review 210

Chapter 9 Understanding EIGRP Concepts 214

Foundation Topics 215
EIGRP and Distance Vector Routing Protocols 215
Introduction to EIGRP 215
Basic Distance Vector Routing Protocol Features 216
The Concept of a Distance and a Vector 216
Full Update Messages and Split Horizon 217
Route Poisoning 219
EIGRP as an Advanced DV Protocol 220
EIGRP Sends Partial Update Messages, As Needed 220
EIGRP Maintains Neighbor Status Using Hello 221
Summary of Interior Routing Protocol Features 221
EIGRP Concepts and Operation 222
EIGRP Neighbors 222
Exchanging EIGRP Topology Information 223
Calculating the Best Routes for the Routing Table 224
The EIGRP Metric Calculation 224
An Example of Calculated EIGRP Metrics 225
Caveats with Bandwidth on Serial Links 226
EIGRP Convergence 227
Feasible Distance and Reported Distance 227
EIGRP Successors and Feasible Successors 228
The Query and Reply Process 229
Chapter Summary 231
Review Questions 231
Chapter Review 233

Chapter 10 Implementing EIGRP for IPv4 234

Foundation Topics 235
Core EIGRP Configuration and Verification 235
EIGRP Configuration 235
Configuring EIGRP Using a Wildcard Mask 236
Verifying EIGRP Core Features 237
Finding the Interfaces on Which EIGRP Is Enabled 238
Displaying EIGRP Neighbor Status 240
Displaying the IPv4 Routing Table 241
EIGRP Metrics, Successors, and Feasible Successors 242
Viewing the EIGRP Topology Table 243
Finding Successor Routes 244
Finding Feasible Successor Routes 245
Convergence Using the Feasible Successor Route 247
Examining the Metric Components 248
Other EIGRP Configuration Settings 249
Load Balancing Across Multiple EIGRP Routes 249
Tuning the EIGRP Metric Calculation 251
Autosummarization and Discontiguous Classful Networks 252
Automatic Summarization at the Boundary of a Classful Network 252
Discontiguous Classful Networks 253
Chapter Summary 255
Review Questions 255
Chapter Review 257

Chapter 11 Troubleshooting IPv4 Routing Protocols 260

Foundation Topics 261
Perspectives on Troubleshooting Routing Protocol Problems 261
Interfaces Enabled with a Routing Protocol 262
EIGRP Interface Troubleshooting 263
Examining Working EIGRP Interfaces 264
Examining the Problems with EIGRP Interfaces 266
OSPF Interface Troubleshooting 268
Neighbor Relationships 270
EIGRP Neighbor Verification Checks 272
EIGRP Neighbor Troubleshooting Example 273
OSPF Neighbor Troubleshooting 274
Finding Area Mismatches 276
Finding Duplicate OSPF Router IDs 277
Finding OSPF Hello and Dead Timer Mismatches 279
Other OSPF Issues 280
Shutting Down the OSPF Process 280
Mismatched MTU Settings 281

Chapter Summary 283
Chapter Review 283

Chapter 12 Implementing External BGP 286

Foundation Topics 287
BGP Concepts 287
Advertising Routes with BGP 287
Internal and External BGP 288
Choosing the Best Routes with BGP 289
eBGP and the Internet Edge 290
Internet Edge Designs and Terminology 290
Advertising the Enterprise Public Prefix into the Internet 291
Learning Default Routes from the ISP 292
eBGP Configuration and Verification 293
BGP Configuration Concepts 294
Configuring eBGP Neighbors Using Link Addresses 294
Verifying eBGP Neighbors 296
Administratively Disabling Neighbors 297
Injecting BGP Table Entries with the network Command 298
Injecting Routes for a Classful Network 298
Advertising Subnets to the ISP 300
Advertising a Single Prefix with a Static Discard Route 301
Learning a Default Route from the ISP 303
Chapter Summary 305
Review Questions 305
Chapter Review 306

Part II Review 310

Part III Wide-Area Networks 313

Chapter 13 Implementing Point-to-Point WANs 314

Foundation Topics 315
Leased-Line WANs with HDLC 315
Layer 1 Leased Lines 315
The Physical Components of a Leased Line 316
The Role of the CSU/DSU 318
Building a WAN Link in a Lab 319
Layer 2 Leased Lines with HDLC 319
Configuring HDLC 320
Leased-Line WANs with PPP 323
PPP Concepts 323
PPP Framing 324
PPP Control Protocols 324
PPP Authentication 325

Implementing PPP 326
Implementing PPP CHAP 327
Implementing PPP PAP 328
Implementing Multilink PPP 330
Multilink PPP Concepts 331
Configuring MLPPP 332
Verifying MLPPP 333
Troubleshooting Serial Links 335
Troubleshooting Layer 1 Problems 335
Troubleshooting Layer 2 Problems 336
Keepalive Failure 336
PAP and CHAP Authentication Failure 337
Troubleshooting Layer 3 Problems 338
Chapter Summary 340
Review Questions 340
Chapter Review 342

Chapter 14 Private WANs with Ethernet and MPLS 346

Foundation Topics 347
Metro Ethernet 347
Metro Ethernet Physical Design and Topology 347
Ethernet WAN Services and Topologies 349
Ethernet Line Service (Point-to-Point) 349
Ethernet LAN Service (Full Mesh) 350
Ethernet Tree Service (Hub and Spoke) 351
Layer 3 Design Using Metro Ethernet 351
Layer 3 Design with E-Line Service 352
Layer 3 Design with E-LAN Service 353
Layer 3 Design with E-Tree Service 353
Ethernet Virtual Circuit Bandwidth Profiles 354
Charging for the Data (Bandwidth) Used 355
Controlling Overages with Policing and Shaping 355
Multiprotocol Label Switching (MPLS) 356
MPLS VPN Physical Design and Topology 358
MPLS and Quality of Service 359
Layer 3 with MPLS VPN 360
OSPF Area Design with MPLS VPN 361
Routing Protocol Challenges with EIGRP 362
Chapter Summary 364
Review Questions 364
Chapter Review 365

Chapter 15 Private WANs with Internet VPN 368

Foundation Topics 369

Internet Access and Internet VPN Fundamentals 369

Internet Access 369

Digital Subscriber Line 370

Cable Internet 371

Wireless WAN (3G, 4G, LTE) 371

Fiber Internet Access 372

Internet VPN Fundamentals 373

Site-to-Site VPNs with IPsec 374

Client VPNs with SSL 375

GRE Tunnels and DMVPN 376

GRE Tunnel Concepts 376

Routing over GRE Tunnels 376

GRE Tunnels over the Unsecured Network 378

Configuring GRE Tunnels 380

Verifying a GRE Tunnel 382

Troubleshooting GRE Tunnels 384

Tunnel Interfaces and Interface State 384

Layer 3 Issues for Tunnel Interfaces 386

Issues with ACLs and Security 387

Multipoint Internet VPNs Using DMVPN 388

PPP over Ethernet 390

PPPoE Concepts 391

PPPoE Configuration 392

PPPoE Configuration Breakdown: Dialers and Layer 1 393

PPPoE Configuration Breakdown: PPP and Layer 2 393

PPPoE Configuration Breakdown: Layer 3 394

PPPoE Configuration Summary 394

A Brief Aside About Lab Experimentation with PPPoE 395

PPPoE Verification 396

Verifying Dialer and Virtual-Access Interface Bindings 397

Verifying Virtual-Access Interface Configuration 398

Verifying PPPoE Session Status 399

Verifying Dialer Interface Layer 3 Status 400

PPPoE Troubleshooting 401

Step 0: Status Before Beginning the First Step 401

Step 1: Status After Layer 1 Configuration 402

Step 2: Status After Layer 2 (PPP) Configuration 403

Step 3: Status After Layer 3 (IP) Configuration 404

PPPoE Troubleshooting Summary 405

Chapter Summary 406
Review Questions 407
Chapter Review 408

Part III Review 412

Part IV IPv4 Services: ACLs and QoS 415

Chapter 16 Basic IPv4 Access Control Lists 416

Foundation Topics 417
IPv4 Access Control List Basics 417
ACL Location and Direction 417
Matching Packets 418
Taking Action When a Match Occurs 418
Types of IP ACLs 419
Standard Numbered IPv4 ACLs 419
List Logic with IP ACLs 419
Matching Logic and Command Syntax 421
Matching the Exact IP Address 421
Matching a Subset of the Address with Wildcards 421
Binary Wildcard Masks 423
Finding the Right Wildcard Mask to Match a Subnet 423
Matching Any/All Addresses 423
Implementing Standard IP ACLs 424
Standard Numbered ACL Example 1 424
Standard Numbered ACL Example 2 426
Troubleshooting and Verification Tips 427
Practice Applying Standard IP ACLs 428
Practice Building access-list Commands 428
Reverse Engineering from ACL to Address Range 429
Chapter Summary 431
Review Questions 431
Chapter Review 432

Chapter 17 Advanced IPv4 Access Control Lists 436

Foundation Topics 437
Extended Numbered IP Access Control Lists 437
Matching the Protocol, Source IP, and Destination IP 437
Matching TCP and UDP Port Numbers 438
Extended IP ACL Configuration 441
Extended IP Access Lists: Example 1 441
Extended IP Access Lists: Example 2 443
Practice Building access-list Commands 444

Named ACLs and ACL Editing 444
Named IP Access Lists 444
Editing ACLs Using Sequence Numbers 446
Numbered ACL Configuration Versus Named ACL Configuration 448
ACL Implementation Considerations 449
Troubleshooting with IPv4 ACLs 450
Analyzing ACL Behavior in a Network 450
ACL Troubleshooting Commands 451
Example Issue: Reversed Source/Destination IP Addresses 452
Steps 3D and 3E: Common Syntax Mistakes 453
Example Issue: Inbound ACL Filters Routing Protocol Packets 454
ACL Interactions with Router-Generated Packets 455
Local ACLs and a Ping from a Router 455
Router Self-Ping of a Serial Interface IPv4 Address 456
Router Self-Ping of an Ethernet Interface IPv4 Address 456
Chapter Summary 458
Review Questions 458
Chapter Review 460

Chapter 18 Quality of Service (QoS) 464

Foundation Topics 465
Introduction to QoS 465
QoS: Managing Bandwidth, Delay, Jitter, and Loss 465
Types of Traffic 466
Data Applications 466
Voice and Video Applications 467
QoS as Mentioned in This Book 468
QoS on Switches and Routers 469
Classification and Marking 469
Classification Basics 469
Matching (Classification) Basics 470
Classification on Routers with ACLs and NBAR 471
Marking IP DSCP and Ethernet CoS 472
Marking the IP Header 472
Marking the Ethernet 802.1Q Header 473
Other Marking Fields 474
Defining Trust Boundaries 474
DiffServ Suggested Marking Values 475
Expedited Forwarding (EF) 475
Assured Forwarding (AF) 475
Class Selector (CS) 476

Congestion Management (Queuing) 476
Round Robin Scheduling (Prioritization) 477
Low Latency Queuing 478
A Prioritization Strategy for Data, Voice, and Video 479
Shaping and Policing 480
Policing 480
Where to Use Policing 481
Shaping 482
Setting a Good Shaping Time Interval for Voice and Video 483
Congestion Avoidance 484
TCP Windowing Basics 484
Congestion Avoidance Tools 485
Chapter Summary 486
Review Questions 486
Chapter Review 487

Part IV Review 490

Part V IPv4 Routing and Troubleshooting 493

Chapter 19 IPv4 Routing in the LAN 494
Foundation Topics 495
VLAN Routing with Router 802.1Q Trunks 495
Configuring ROAS 496
Verifying ROAS 498
Troubleshooting ROAS 500
VLAN Routing with Layer 3 Switch SVIs 501
Configuring Routing Using Switch SVIs 501
Verifying Routing with SVIs 502
Troubleshooting Routing with SVIs 503
VLAN Routing with Layer 3 Switch Routed Ports 505
Implementing Routed Interfaces on Switches 506
Implementing Layer 3 EtherChannels 508
Troubleshooting Layer 3 EtherChannels 511
Chapter Summary 512
Review Questions 512
Chapter Review 514

Chapter 20 Implementing HSRP for First-Hop Routing 516
Foundation Topics 517
FHRP and HSRP Concepts 517
The Need for Redundancy in Networks 517
The Need for a First Hop Redundancy Protocol 519
The Three Solutions for First-Hop Redundancy 520

HSRP Concepts 521
HSRP Failover 521
HSRP Load Balancing 522
Implementing HSRP 523
Configuring and Verifying Basic HSRP 523
HSRP Active Role with Priority and Preemption 526
HSRP Versions 528
Troubleshooting HSRP 528
Checking HSRP Configuration 529
Symptoms of HSRP Misconfiguration 530
Chapter Summary 532
Review Questions 533
Chapter Review 534

Chapter 21 Troubleshooting IPv4 Routing 536

Foundation Topics 537
Problems Between the Host and the Default Router 537
Root Causes Based on a Host's IPv4 Settings 537
Ensure IPv4 Settings Correctly Match 537
Mismatched Masks Impact Route to Reach Subnet 538
Typical Root Causes of DNS Problems 540
Wrong Default Router IP Address Setting 541
Root Causes Based on the Default Router's Configuration 541
DHCP Issues 542
Router LAN Interface and LAN Issues 543
Problems with Routing Packets Between Routers 545
IP Forwarding by Matching the Most Specific Route 545
Using show ip route and Subnet Math to Find the Best Route 546
Using show ip route *address* to Find the Best Route 547
show ip route Reference 548
Routing Problems Caused by Incorrect Addressing Plans 549
Recognizing When VLSM Is Used or Not 549
Overlaps When Not Using VLSM 549
Overlaps When Using VLSM 550
Configuring Overlapping VLSM Subnets 551
Pointers to Related Troubleshooting Topics 552
Router WAN Interface Status 552
Filtering Packets with Access Lists 553
Chapter Summary 554
Chapter Review 554

Part V Review 556

Part VI IPv6 561

Chapter 22 IPv6 Routing Operation and Troubleshooting 562

Foundation Topics 563
Normal IPv6 Operation 563
Unicast IPv6 Addresses and IPv6 Subnetting 563
Assigning Addresses to Hosts 565
Stateful DHCPv6 565
Stateless Address Autoconfiguration 566
Router Address and Static Route Configuration 567
Configuring IPv6 Routing and Addresses on Routers 567
IPv6 Static Routes on Routers 568
Verifying IPv6 Connectivity 569
Verifying Connectivity from IPv6 Hosts 569
Verifying IPv6 from Routers 571
Troubleshooting IPv6 572
Pings from the Host Work Only in Some Cases 573
Pings Fail from a Host to Its Default Router 574
Problems Using Any Function That Requires DNS 575
Host Is Missing IPv6 Settings: Stateful DHCP Issues 576
Host Is Missing IPv6 Settings: SLAAC Issues 577
Traceroute Shows Some Hops, But Fails 579
Routing Looks Good, But Traceroute Still Fails 580
Chapter Summary 581
Chapter Review 582

Chapter 23 Implementing OSPF for IPv6 584

Foundation Topics 585
OSPFv3 for IPv6 Concepts 585
IPv6 Routing Protocol Versions and Protocols 585
Two Options for Implementing Dual Stack with OSPF 585
OSPFv2 and OSPFv3 Internals 586
OSPFv3 Configuration 587
Basic OSPFv3 Configuration 587
Single-Area Configuration on the Three Internal Routers 589
Adding Multiarea Configuration on the Area Border Router 590
Other OSPFv3 Configuration Settings 591
Setting OSPFv3 Interface Cost to Influence Route Selection 591
OSPF Load Balancing 592
Injecting Default Routes 593
OSPFv3 Verification and Troubleshooting 593
OSPFv3 Interfaces 595
Verifying OSPFv3 Interfaces 595
Troubleshooting OSPFv3 Interfaces 596

OSPFv3 Neighbors 597
Verifying OSPFv3 Neighbors 597
Troubleshooting OSPFv3 Neighbors 598
OSPFv3 LSDB and LSAs 600
The Issue of IPv6 MTU 601
OSPFv3 Metrics and IPv6 Routes 602
Verifying OSPFv3 Interface Cost and Metrics 602
Troubleshooting IPv6 Routes Added by OSPFv3 604
Chapter Summary 606
Review Questions 607
Chapter Review 608

Chapter 24 Implementing EIGRP for IPv6 612
Foundation Topics 613
EIGRP for IPv6 Configuration 613
EIGRP for IPv6 Configuration Basics 613
EIGRP for IPv6 Configuration Example 614
Other EIGRP for IPv6 Configuration Settings 616
Setting Bandwidth and Delay to Influence EIGRP for IPv6 Route Selection 616
EIGRP Load Balancing 617
EIGRP Timers 618
EIGRP for IPv6 Verification and Troubleshooting 619
EIGRP for IPv6 Interfaces 620
EIGRP for IPv6 Neighbors 621
EIGRP for IPv6 Topology Database 623
EIGRP for IPv6 Routes 624
Chapter Summary 627
Review Questions 627
Chapter Review 629

Chapter 25 IPv6 Access Control Lists 632
Foundation Topics 633
IPv6 Access Control List Basics 633
Similarities and Differences Between IPv4 and IPv6 ACLs 633
ACL Location and Direction 634
IPv6 Filtering Policies 634
ICMPv6 Filtering Caution 635
Capabilities of IPv6 ACLs 635
Limitations of IPv6 ACLs 636
Matching Tunneled Traffic 636
IPv4 Wildcard Mask and IPv6 Prefix Length 636
ACL Logging Impact 636
Router Originated Packets 637

Configuring Standard IPv6 ACLs 637
Configuring Extended IPv6 ACLs 640
Examples of Extended IPv6 ACLs 642
Practice Building ipv6 access-list Commands 644
Other IPv6 ACL Topics 644
Implicit IPv6 ACL Rules 644
An Example of Filtering ICMPv6 NDP and the Negative Effects 645
How to Avoid Filtering ICMPv6 NDP Messages 648
IPv6 ACL Implicit Filtering Summary 649
IPv6 Management Control ACLs 649
Chapter Summary 651
Review Questions 651
Chapter Review 652

Part VI Review 656

Part VII Miscellaneous 659

Chapter 26 Network Management 660
Foundation Topics 661
Simple Network Management Protocol 661
SNMP Concepts 661
SNMP Variable Reading and Writing: SNMP Get and Set 661
SNMP Notifications: Traps and Informs 662
The Management Information Base 663
Securing SNMP 664
Implementing SNMP Version 2c 665
Configuring SNMPv2c Support for Get and Set 665
Configuring SNMPv2c Support for Trap and Inform 666
Verifying SNMPv2c Operation 667
Implementing SNMP Version 3 669
SNMPv3 Groups 669
SNMPv3 Users, Passwords, and Encryption Keys 671
Verifying SNMPv3 673
Implementing SNMPv3 Notifications (Traps and Informs) 674
Summarizing SNMPv3 Configuration 675
IP Service Level Agreement 676
An Overview of IP SLA 677
Basic IP SLA ICMP-Echo Configuration 678
Troubleshooting Using IP SLA Counters 678
Troubleshooting Using IP SLA History 680

SPAN 681
SPAN Concepts 681
The Need for SPAN When Using a Network Analyzer 682
SPAN Session Concepts 683
Configuring Local SPAN 684
SPAN Session Parameters for Troubleshooting 687
Choosing to Limit SPAN Sources 687
Chapter Summary 689
Review Questions 690
Chapter Review 691

Chapter 27 Cloud Computing 696

Foundation Topics 697
Cloud Computing Concepts 697
Server Virtualization 697
Cisco Server Hardware 697
Server Virtualization Basics 698
Networking with Virtual Switches on a Virtualized Host 699
The Physical Data Center Network 700
Workflow with a Virtualized Data Center 701
Cloud Computing Services 702
Private Cloud 703
Public Cloud 704
Cloud and the "As a Service" Model 705
Infrastructure as a Service 705
Software as a Service 706
(Development) Platform as a Service 706
WAN Traffic Paths to Reach Cloud Services 707
Enterprise WAN Connections to Public Cloud 707
Accessing Public Cloud Services Using the Internet 707
Pros and Cons with Connecting to Public Cloud with Internet 708
Private WAN and Internet VPN Access to Public Cloud 709
Pros and Cons with Connecting to Cloud with Private WANs 710
Intercloud Exchanges 710
Summarizing the Pros and Cons of Public Cloud WAN Options 711
A Scenario: Branch Offices and the Public Cloud 711
Migrating Traffic Flows When Migrating to Email SaaS 712
Branch Offices with Internet and Private WAN 713
Virtual Network Functions and Services 714
Virtual Network Functions: Firewalls and Routers 714
DNS Services 716
Address Assignment Services and DHCP 717
NTP 718

Chapter Summary 720
Review Questions 720
Chapter Review 721

Chapter 28 SDN and Network Programmability 724

Foundation Topics 725
SDN and Network Programmability Basics 725
The Data, Control, and Management Planes 725
The Data Plane 725
The Control Plane 726
The Management Plane 727
Cisco Switch Data Plane Internals 727
Controllers and Network Architecture 728
Controllers and Centralized Control 728
The Southbound Interface 729
The Northbound Interface 730
SDN Architecture Summary 732
Examples of Network Programmability and SDN 732
Open SDN and OpenFlow 732
The OpenDaylight Controller 733
Cisco Open SDN Controller 734
The Cisco Application Centric Infrastructure 734
The Cisco APIC Enterprise Module 735
Comparing the Three Examples 737
Cisco APIC-EM Path Trace ACL Analysis Application 738
APIC-EM Path Trace App 738
APIC-EM Path Trace ACL Analysis Tool Timing and Exam Topic 738
Chapter Summary 740
Review Questions 741
Chapter Review 741

Part VII Review 744

Part VIII Final Prep 747

Chapter 29 Final Review 748

Advice About the Exam Event 748
Learn the Question Types Using the Cisco Certification Exam Tutorial 748
Think About Your Time Budget Versus Number of Questions 749
A Suggested Time-Check Method 750
Miscellaneous Pre-Exam Suggestions 750
Exam-Day Advice 750
Reserve the Hour After the Exam in Case You Fail 751
Exam Review 752

Take Practice Exams 752
Practicing Taking the ICND2 or CCNA R&S Exam 753
Advice on How to Answer Exam Questions 753
Taking Other Practice Exams 755
Find Knowledge Gaps Through Question Review 755
Practice Hands-On CLI Skills 757
Review Mind Maps from Part Review 757
Do Labs 757
Assess Whether You Are Ready to Pass (and the Fallacy of Exam Scores) 759
Study Suggestions After Failing to Pass 759
Other Study Tasks 760
Final Thoughts 761

Part IX Appendixes 763

Appendix A Numeric Reference Tables 764

Appendix B CCNA ICND2 200-105 Exam Updates 770

Glossary 780

Index 816

DVD Appendixes

Appendix C Answers to the Review Questions

Appendix D Practice for Chapter 16: Basic IPv4 Access Control Lists

Appendix E Mind Map Solutions

Appendix F Study Planner

Appendix G Learning IPv4 Routes with RIPv2

Appendix H Understanding Frame Relay Concepts

Appendix I Implementing Frame Relay

Appendix J IPv4 Troubleshooting Tools

Appendix K Topics from Previous Editions

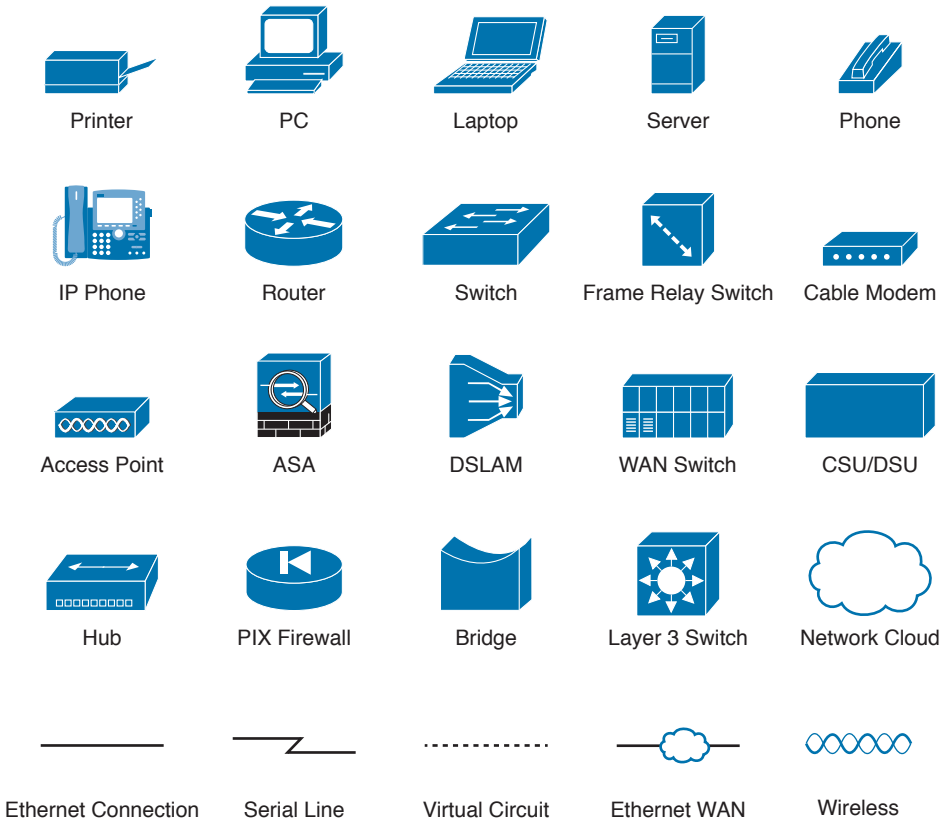
Appendix L Exam Topic Cross Reference

Reader Services

To access additional content for this book, simply register your product. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587205989 and click Submit. After the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Icons Used in This Book



Command Syntax Conventions

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

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

About the 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 to Achieve CCENT and CCNA R&S

Cisco announced changes to the CCENT and CCNA Routing and Switching certifications, and the related 100-105 ICND1, 200-105 ICND2, and 200-125 CCNA exams, early in the year 2016. Most everyone new to Cisco certifications begins with either CCENT or CCNA Routing and Switching (CCNA R&S). However, the paths to certification are not quite obvious at first.

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

Cisco gives you two options to achieve CCNA R&S certification, as shown in Figure I-1: pass both the ICND1 and ICND2 exams, or just pass the CCNA exam. Both paths cover the same exam topics, but the two-exam path does so spread over two exams rather than one. You also pick up the CCENT certification by going through the two-exam path, but you do not when working through the single-exam (200-125) option.

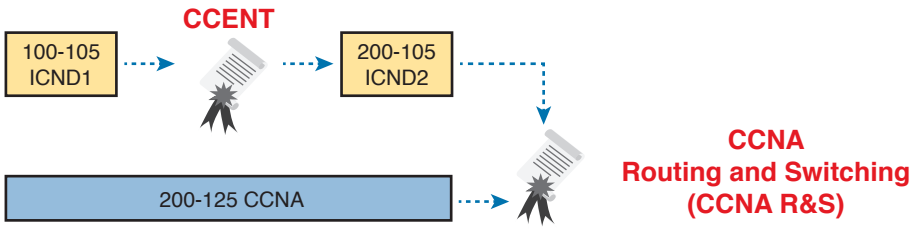


Figure I-1 *Cisco Entry-Level Certifications and Exams*

Note that Cisco has begun referencing some exams with a version number on some of their web-sites. If that form holds true, the exams in Figure I-1 will likely be called version 3 (or v3 for short). Historically, the 200-125 CCNA R&S exam is the seventh separate version of the exam (which warrants a different exam number), dating back to 1998. To make sure you reference the correct exam, when looking for information, using forums, and registering for the test, just make sure to use the correct exam number as shown in the figure.

Types of Questions on the Exams

The ICND1, ICND2, and CCNA R&S 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. The question types are

- Multiple-choice, single-answer
- Multiple-choice, multiple-answer
- Testlet (one scenario with several multiple-choice questions)
- Drag-and-drop

- Simulated lab (sim)
- Simlet

You should take the time to learn as much as possible by using the Cisco Certification Exam Tutorial, which you can find by going to Cisco.com and searching for "exam tutorial." This tool walks through each type of question Cisco may ask on the exam.

Although the first four types of questions in the list should be familiar to anyone who has taken standardized tests or similar tests in school, the last two types are more common to IT tests and Cisco exams in particular. Both use a network simulator to ask questions, so that you control and use simulated Cisco devices. In particular:

- **Sim questions:** You see a network topology, a lab scenario, and can access the devices. Your job is to fix a problem with the configuration.
- **Simlet questions:** This style combines sim and testlet question formats. Like a sim question, you see a network topology, a lab scenario, and can access the devices. However, like a testlet, you also see several multiple-choice questions. Instead of changing/fixing the configuration, you answer questions about the current state of the network.

Using these two question styles with the simulator enables Cisco to test your configuration skills with sim questions, and your verification and troubleshooting skills with simlet questions.

What's on the CCNA Exams…and in the Book?

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.

You can find out more about what's on the exam from two primary sources: this book and the Cisco website.

The Cisco Published Exam Topics

First, Cisco tells the world the specific topics on each of their certification exams. For every Cisco certification exam, Cisco wants the public to know both the variety of topics and what kinds of knowledge and skills are required for each topic. Just go to http://www.cisco.com/go/certifications, look for the CCENT and CCNA Routing and Switching pages, and navigate until you see the exam topics.

Note that this book lists those same exam topics in Appendix L, "Exam Topic Cross Reference." This PDF appendix lists two cross references: one with a list of the exam topics in the order in which Cisco lists them on their website; and the other with a list of chapters in this book with the corresponding exam topics included in each chapter.

Cisco does more than just list the topic (for example, IPv4 addressing); they also list the depth to which you must master the topic. The primary exam topics each list one or more verbs that describe the skill level required. For example, consider the following exam topic, which describes one of the most important topics in both CCENT and CCNA R&S:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

Note that this one exam topic has three verbs (configure, verify, and troubleshoot). So, you should be able to not only configure IPv4 addresses and subnets, but also understand them well enough to verify that the configuration works, and to troubleshoot problems when it is not working. And if to do that you need to understand concepts and need to have other knowledge, those details are implied. The exam questions will attempt to assess whether you can configure, verify, and troubleshoot.

The Cisco exam topics provide the definitive list of topics and skill levels required by Cisco for the exams. But the list of exam topics provides only a certain level of depth. For example, the ICND1 100-105 exam topics list has 41 primary exam topics (topics with verbs), plus additional subtopics that provide more details about that technology area. Although very useful, the list of exam topics would take about five pages of this book if laid out in a list.

You should take the time to not only read the exam topics, but read the short material above the exam topics as listed at the Cisco web page for each certification and exam. Look for notices about the use of unscored items, and how Cisco intends the exam topics to be a set of general guidelines for the exams.

This Book: About the Exam Topics

This book provides a complete study system for the Cisco published exam topics for the ICND2 200-105 exam. All the topics in this book either directly relate to some ICND2 exam topic or provide more basic background knowledge for some exam topic. The scope of the book is defined by the exam topics.

For those of you thinking more specifically about the CCNA R&S certification, and the CCNA 200-125 single-exam path to CCNA, this book covers about one-half of the CCNA exam topics. The *CCENT/CCNA ICND1 100-105 Official Cert Guide* (and ICND1 100-105 exam topics) covers about half of the topics listed for the CCNA 200-125 exam, and this book (and the ICND2 200-105 exam topics) covers the other half. In short, for content, CCNA = ICND1 + ICND2.

Book Features

This book (and the related *CCENT/CCNA ICND1 100-105 Official Cert Guide*) goes beyond what you would find in a simple technology book. It gives you a study system designed to help you not only learn facts but also to develop the skills you need to pass the exams. To do that, in the technology chapters of the book, about three-quarters of the chapter is about the technology, and about one-quarter is for the related study features.

The "Foundation Topics" section of each chapter contains rich content to explain the topics on the exam and to show many examples. This section makes extensive use of figures, with lists and tables for comparisons. It also highlights the most important topics in each chapter as key topics, so you know what to master first in your study.

Most of the book's features tie in some way to the need to study beyond simply reading the "Foundation Topics" section of each chapter. The rest of this section explains these book features. And because the book organizes your study by chapter, and then by part (a part contains multiple chapters), and then a final review at the end of the book, the next section of this Introduction discusses the book features introduced by chapter, part, and for final review.

Chapter Features and How to Use Each Chapter

Each chapter of this book is a self-contained short course about one topic area, organized for reading and study as follows:

- **Foundation Topics:** This is the heading for the core content section of the chapter.
- **Chapter Review:** This section includes a list of study tasks useful to help you remember concepts, connect ideas, and practice skills-based content in the chapter.

In addition to these two main chapter features, each "Chapter Review" section presents a variety of other book features, including the following:

- **Review Key Topics:** In the "Foundation Topics" section, the Key Topic icon appears next to the most important items, for the purpose of later review and mastery. While all content

matters, some is, of course, more important to learn, or needs more review to master, so these items are noted as key topics. The "Review Key Topics" section lists the key topics in a table; scan the chapter for these items to review them.

- **Chapter Summary:** This section provides a list of the key concepts covered in each chapter for quick reference and review.
- **Review Questions:** These questions help you test your understanding of the material covered in each chapter.
- **Complete Tables from Memory:** Instead of just rereading an important table of information, some tables have been marked as memory tables. These tables exist in the Memory Table app that is available on the DVD and from the companion website. The app shows the table with some content removed, and then reveals the completed table, so you can work on memorizing the content.
- **Key Terms You Should Know:** You do not need to be able to write a formal definition of all terms from scratch. However, you do need to understand each term well enough to understand exam questions and answers. This section lists the key terminology from the chapter. Make sure you have a good understanding of each term, and use the DVD Glossary to cross-check your own mental definitions.
- **Labs:** Many exam topics use the verbs "configure," "verify," and "troubleshoot"; all these refer to skills you should practice at the command-line interface (CLI) of a router or switch. The Chapter Review refers you to these other tools. The Introduction's section titled "About Building Hands-On Skills" discusses your options.
- **Command References:** Some book chapters cover a large number of router and switch commands. This section includes reference tables for the commands used in that chapter, along with an explanation. Use these tables for reference, but also use them for study—just cover one column of the table, and see how much you can remember and complete mentally.

Part Features and How to Use Part Review

The book organizes the chapters into seven parts. Each part contains a number of related chapters. Figure I-2 lists the titles of the parts and identifies the chapters in those parts by chapter numbers.

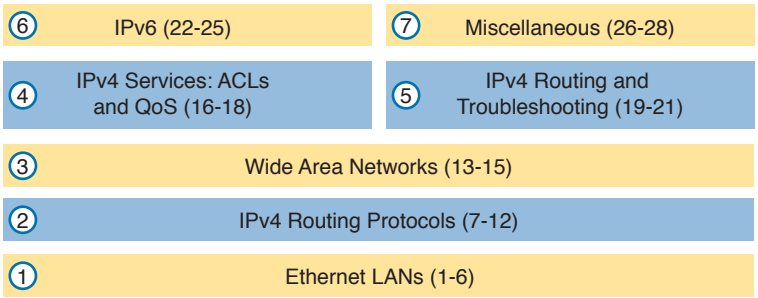


Figure I-2 *The Book Parts and Corresponding Chapter Numbers*

Each book part ends with a "Part Review" section that contains a list of activities for study and review, much like the "Chapter Review" section at the end of each chapter. However, because the Part Review takes place after completing a number of chapters, the Part Review includes some tasks meant to help pull the ideas together from this larger body of work. The following list explains the types of tasks added to each Part Review beyond the types mentioned for the Chapter Review:

- **Answer Part Review Questions:** The books come with exam software and databases of questions. One database holds questions written specifically for Part Reviews. These questions tend to connect multiple ideas together, to help you think about topics from multiple chapters, and to build the skills needed for the more challenging analysis questions on the exams.

- **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. The Part Review elements make use of mind maps in several ways: to connect concepts and the related configuration commands, to connect **show** commands and the related networking concepts, and even to connect terminology. (For more information about mind maps, see the section "About Mind Maps" later in this Introduction.)
- **Labs:** Each "Part Review" section will direct you to the kinds of lab exercises you should do with your chosen lab product, labs that would be more appropriate for this stage of study and review. (Check out the later section "About Building Hands-On Skills" for information about lab options.)

In addition to these tasks, many "Part Review" sections have you perform other tasks with book features mentioned in the "Chapter Review" section: repeating chapter review quiz questions, reviewing key topics, and doing more lab exercises.

Final Review

Chapter 29, "Final Review," lists a series of preparation tasks that you can best use for your final preparation before taking the exam. Chapter 29 focuses on a three-part approach to helping you pass: practicing your skills, practicing answering exam questions, and uncovering your weak spots. To that end, Chapter 29 uses the same familiar book features discussed for the Chapter Review and Part Review elements, along with a much larger set of practice questions.

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:

- **Premium Edition Practice Test:** This Academic Edition comes with a free version of the Premium Edition Practice Test. To access this test, you will need to redeem the digital product voucher listed on the card in the DVD sleeve in the back of this book. You can take simulated ICND2 exams, as well as CCNA exams, with the Premium Edition Practice Test activation code you will get when you redeem the digital product voucher on our website. (You can take simulated ICND1 and CCNA R&S exams with the DVD in the *CCENT/CCNA ICND1 100-105 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 CLI. No need to go buy real gear or buy a full simulator to start learning the CLI. Just install it from the DVD in the back of this book.
- **eBook:** This Academic Edition comes complete with three free eBook files. To access these files, you will need to redeem the Premium Edition eBook and Practice Test digital product voucher code found on the access card in the DVD sleeve. This will give you access to the PDF, EPUB, and Kindle versions of the eBook.
- **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/9781587205989 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:** I maintain a website that hosts tools and links that are 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 my CCENT Skills blog and CCNA Skills blog. Start at http://www.certskills.com; click the Blog tab for a page about the blogs in particular, with links to the pages with the labs related to this book.

A Big New Feature: Review Applications

One of the single biggest new features of this edition of the book is the addition of study apps for many of the Chapter Review activities. In the past, all Chapter Review activities used only the book chapter, or the chapter plus a DVD-only appendix. Readers tell us they find that content useful, but the content is static.

This book and the *CCENT/CCNA ICND1 100-105 Official Cert Guide* are the first Cisco Press Cert Guides with extensive interactive applications. Basically, most every activity that can be done in the "Chapter Review" sections can now be done with an application. The apps can be found both on the DVD that comes with the book and on the book's companion website. On the DVD you can find the apps under the "Chapter and Part Review" tab.

The advantages of using these apps are as follows:

- **Easier to use:** Instead of having to print out copies of the appendixes and do the work on paper, these new apps provide you with an easy-to-use, interactive experience that you can easily run over and over.
- **Convenient:** When you have a spare 5–10 minutes, go to the book's website, and review content from one of your recently finished chapters.
- **Untethered from book/DVD:** Because these apps are available on the book's companion website in addition to the DVD, you can access your review activities from anywhere—no need to have the book or DVD with you.
- **Good for tactile learners:** Sometimes looking at a static page after reading a chapter lets your mind wander. Tactile learners may do better by at least typing answers into an app, or clicking inside an app to navigate, to help keep you focused on the activity.

Our in-depth reader surveys show that readers who use the Chapter Review tools like them, but that not everyone uses them consistently. So, we want to increase the number of people using the review tools, and make them both more useful and more interesting. Table I-1 summarizes these new applications and the traditional book features that cover the same content.

Table I-1 Book Features with Both Traditional and App Options

Feature	Traditional	App
Key Topics	Table with list; flip pages to find	Key Topics Table app
Config Checklist	Just one of many types of key topics	Config Checklist app
Memory Table	Two static PDF appendixes (one with sparse tables for you to complete, one with completed tables)	Memory Table app

Feature	Traditional	App
Key Terms	Listed in each "Chapter Review" section, with the Glossary in the back of the book	Glossary Flash Cards app
IPv4 ACL Practice	A static PDF appendix (D) with practice problems	An interactive app that asks the same problems as listed in the appendix

How to Get the Electronic Elements of This Book

Traditionally, all chapter review activities use the book chapter plus appendixes, with the appendixes often being located on the DVD. But most of that content is static—useful, but static.

If you buy the print book, and have a DVD drive, you have all the content on the DVD. Just spin the DVD and use the disk menu (which should automatically start) to explore all the content.

If you buy the print book but do not have a DVD drive, you can get the DVD files by redeeming your Premium Edition eBook and Practice Test digital product voucher code on our website. After you have redeemed this product, your book will automatically be registered on your account page. Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book's companion website.

Book Organization, Chapters, and Appendixes

This book contains 28 core chapters, Chapters 1 through 28, with Chapter 29 as the "Final Review" chapter. 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: Ethernet LANs

- **Chapter 1, "Implementing Ethernet Virtual LANs,"** explains the concepts and configuration surrounding virtual LANs, including VLAN trunking.
- **Chapter 2, "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 3, "Spanning Tree Protocol Implementation,"** shows how to configure and verify STP on Cisco switches.
- **Chapter 4, "LAN Troubleshooting,"** examines the most common LAN switching issues and how to discover those issues when troubleshooting a network. The chapter includes troubleshooting topics for STP/RSTP, Layer 2 EtherChannel, LAN switching, VLANs, and VLAN trunking.
- **Chapter 5, "VLAN Trunking Protocol,"** shows how to configure, verify, and troubleshoot the use of VLAN Trunking Protocol (VTP) to define and advertise VLANs across multiple Cisco switches.
- **Chapter 6, "Miscellaneous LAN Topics,"** as the last chapter in the book specifically about LANs, discusses a variety of small topics, including: 802.1x, AAA authentication, DHCP snooping, switch stacking, and chassis aggregation.

Part II: IPv4 Routing Protocols

- **Chapter 7, "Understanding OSPF Concepts,"** introduces the fundamental operation of the Open Shortest Path First (OSPF) protocol, focusing on link state fundamentals, neighbor relationships, flooding link state data, and calculating routes based on the lowest cost metric.
- **Chapter 8, "Implementing OSPF for IPv4,"** takes the concepts discussed in the previous chapter and shows how to configure and verify those same features.

- **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 EIGRP 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.
- **Chapter 12, "Implementing External BGP,"** examines the basics of the Border Gateway Protocol (BGP) and its use between an enterprise and an ISP, showing how to configure, verify, and troubleshoot BGP in limited designs.

Part III: Wide Area Networks

- **Chapter 13, "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 14, "Private WANs with Ethernet and MPLS,"** explores the concepts behind building a WAN service using Ethernet through different Metro Ethernet services, as well as using Multiprotocol Label Switching (MPLS) VPNs.
- **Chapter 15, "Private WANs with Internet VPNs,"** works through a variety of conceptual material, plus some configuration and verification topics, for several technologies related to using the Internet to create a private WAN connection between different enterprise sites.

Part IV: IPv4 Services: ACLs and QoS

- **Chapter 16, "Basic IPv4 Access Control Lists,"** examines how standard IP ACLs can filter packets based on the source IP address so that a router will not forward the packet.
- **Chapter 17, "Advanced IPv4 Access Control Lists,"** examines both named and numbered ACLs, and both standard and extended IP ACLs.
- **Chapter 18, "Quality of Service (QoS),"** discusses a wide variety of concepts all related to the broad topic of QoS.

Part V: IPv4 Routing and Troubleshooting

- **Chapter 19, "IPv4 Routing in the LAN,"** shows to a configuration and troubleshooting depth different methods to route between VLANs, including Router on a Stick (ROAS), Layer 3 switching with SVIs, Layer 3 switching with routed ports, and using Layer 3 EtherChannels.
- **Chapter 20, "Implementing HSRP for First-Hop Routing,"** discusses the need for a First Hop Redundancy Protocol (FHRP), and specifically how to configure, verify, and troubleshoot Hot Standby Router Protocol (HSRP)
- **Chapter 21, "Troubleshooting IPv4 Routing,"** looks at the most common IPv4 problems and how to find the root causes of those problems when troubleshooting.

Part VI: IPv6

- **Chapter 22, "IPv6 Routing Operation and Troubleshooting,"** 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 23, "Implementing OSPF for IPv6,"** explores OSPFv3 and its use as an IPv6 routing protocol, showing traditional configuration, verification, and troubleshooting topics.

- **Chapter 24, "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. It then shows how to configure, verify, and troubleshoot EIGRP for IPv6.
- **Chapter 25, "IPv6 Access Control Lists,"** examines the similarities and differences between IPv4 ACLs and IPv6 ACLs, then shows how to configure, verify, and troubleshoot IPv6 ACLs.

Part VII: Miscellaneous

- **Chapter 26, "Network Management,"** discusses several network management topics that Cisco did not choose to put into ICND1, namely: SNMP, IP SLA, and SPAN.
- **Chapter 27, "Cloud Computing,"** is one of two chapters about topics that strays from traditional CCNA R&S topics as one of the Cisco emerging technology topics. This chapter explains the basic concepts and then generally discusses the impact that cloud computing has on a typical enterprise network.
- **Chapter 28, "SDN and Network Programmability,"** is the other chapter that moves away from traditional CCNA R&S topics to discuss many concepts and terms related to how Software Defined Networking (SDN) and network programmability are impacting typical enterprise networks.

Part VIII: Final Prep

- **Chapter 29, "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 IX: 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, "CCNA ICND2 200-105 Exam Updates,"** is a place for the author to add book content mid-edition. Always check online for the latest PDF version of this appendix; the appendix lists download instructions.
- The **Glossary** contains definitions for all of the terms listed in the "Key Terms You Should Know" sections at the conclusion of Chapters 1 through 28.

Part X: DVD Appendixes

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

- **Appendix C, "Answers to the Chapter Review Quizzes,"** includes the explanations to all the questions from Chapters 1 through 28.
- **Appendix D, "Practice for Chapter 16: Basic IPv4 Access Control Lists,"** is a copy of the *CCENT/CCNA ICND1 100-105 Official Cert Guide*'s Appendix I.
- **Appendix E, "Mind Map Solutions,"** shows an image of sample answers for all the part-ending mind map exercises.
- **Appendix F, "Study Planner,"** is a spreadsheet with major study milestones, where you can track your progress through your study.
- **Appendix G, "Learning IPv4 Routes with RIPv2,"** explains how routers work together to find all the best routes to each subnet using a routing protocol. This chapter also shows how to configure the RIPv2 routing protocol for use with IPv4. (This appendix is a copy of ICND1's Chapter 19, and is included with the ICND2 book for convenience.)
- **Appendix H, "Understanding Frame Relay Concepts,"** explains how to build a Frame Relay WAN between routers, focusing on the protocols and concepts rather than the configuration. (This chapter is a chapter that covers old exam topics from the previous edition of the book, included here for those who might be interested.)

- **Appendix I, "Implementing Frame Relay,"** takes the concepts discussed in Appendix H and shows how to configure, verify, and troubleshoot those same features. (This chapter is a chapter that covers old exam topics from the previous edition of the book, included here for those who might be interested.)
- **Appendix J, "IPv4 Troubleshooting Tools,"** focuses on how to use two key troubleshooting tools to find routing problems: the **ping** and **traceroute** commands. (This appendix is a copy of ICND1's Chapter 23, and is included with the ICND2 book for convenience.)
- **Appendix K, "Topics from Previous Editions,"** is a collection of information about topics that have appeared on previous versions of the CCNA exams. While you most likely will not encounter exam questions on these topics, the concepts are still of interest to someone with the CCENT or CCNA certification.
- **Appendix L, "Exam Topic Cross Reference,"** provides some tables to help you find where each exam objective is covered in the book.

ICND1 Chapters in this Book

For this current edition of the ICND1 and ICND2 Cert Guides, I designed several chapters to be used in both books. These chapters include some topics that are listed in the exam topics of both exams:

- Chapter 1, "Implementing Ethernet Virtual LANs" (Chapter 11 in the ICND1 100-105 book).
- Chapter 16, "Basic IPv4 Access Control Lists" (Chapter 25 in the ICND1 100-105 book).
- Chapter 17, "Advanced IPv4 Access Control Lists" (Chapter 26 in the ICND1 100-105 book).
- Chapter 21, "Troubleshooting IPv4 Routing" (Chapter 24 in the ICND1 100-105 book).

I designed these four chapters for use in both books to be a help to those reading both books while avoiding any problems for those who might be reading only this ICND2 Cert Guide. Cisco has traditionally had some topics that overlap between the two exams that make up the two-exam path to CCNA R&S, and this current pair of exams is no exception. So, for those of you who have already read the ICND1 100-105 book, you can move more quickly through the above four chapters in this book. If you did not read the ICND1 100-105 book, then you have all the material you need right here in this book.

Extra Content Found in DVD Appendixes

Note that several appendixes on the DVD, namely G, H, I, J, and K, contain extra content outside the ICND2 200-105 exam topics. This short section explains why.

First, two appendixes are here to aid the transition when Cisco announced the exams. Appendixes G (about RIP) and J (about **ping** and **traceroute**) are copies of two chapters in the ICND1 100-105 book, and are part of the exam topics for the ICND1 100-105 exam. These two chapters might be particularly useful for anyone who was far along in their studies on the date when Cisco announced the ICND1 100-105 and ICND2 200-105 exams in 2016. I included Appendixes G and J to aid that transition for those who buy the ICND2 200-105 Cert Guide but not the ICND1 100-105 Cert Guide.

Three other appendixes are included for instructors who use these books for classes, as well as for the occasional reader who is mostly interested in the technology instead of the certification. Appendixes H, I, and K contain content that is no longer mentioned by the exam topics for the current exams. Appendixes H and I are copies of complete chapters about Frame Relay from the prior edition of this book, and Appendix K is a compilation of small topics I removed from the prior edition of this book when creating this current edition. This material might be helpful to some instructors during the transition time for their courses, or for those who want to read more broadly just for the sake of learning.

You do not need to use these extra appendixes (G through K) to prepare for the ICND2 200-105 exam or the CCNA R&S 200-125 exam, but feel free to use them if you are interested.

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

This book, like many other Cisco Press books, includes the rights to use the Pearson IT Certification Practice Test (PCPT) software, along with rights to use some exam questions related to this book. PCPT has many options, including the option to answer questions in study mode, so you can see the answers and explanations for each question as you go along; the option to take a simulated exam that mimics real exam conditions; and the option to view questions in flash card mode, where all the answers are stripped out, challenging you to answer questions from memory.

You should install PCPT so it is ready to use even for the earliest chapters. This book's Part Review sections ask you specifically to use PCPT, and you can even take the book chapter quizzes using PCPT.

NOTE The right to use the exams associated with this book is based on an activation code. Redeeming the Premium Edition eBook and Practice Test digital product voucher code in this book will automatically populate your account page with the PCPT software activation code you need to unlock your exams. *Do not lose the activation code.*

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-3.

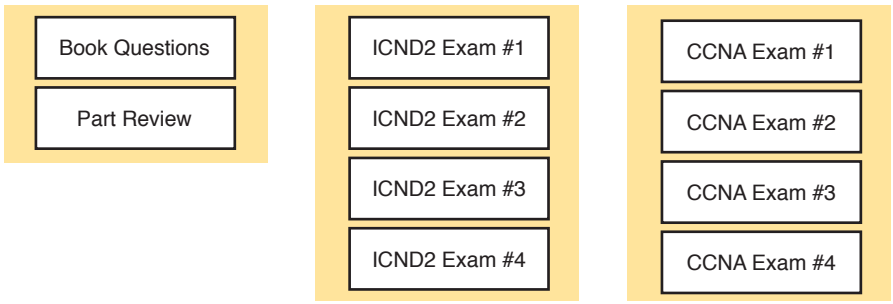


Figure I-3 *PCPT Exams/Exam Databases and When to Use Them*

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-3 begins to suggest a plan, spelled out here:

- During Part Review, use PCPT to review the book 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 the "Final Review" chapter at the end of the book; if preparing for the ICND2 exam, use those practice exams, but if preparing for the CCNA exam, use those exams.

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.

PCPT practice mode lets you practice an exam 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 Part Review Questions

The exam databases you get with this book include a database of questions created solely for study during the Part Review process. Book questions focus more on facts, to help you determine whether you know the facts contained within the chapter. The Part Review questions instead focus more on application of those facts to typical real scenarios, and look more like real exam questions.

To view these questions, follow the same process as you did with book questions, but select the Part Review database rather than the book database. PCPT has a clear name for this database: Part Review 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 improve your brain's 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 and create new connections, all into your own frame of reference.

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

Each mind map begins with a blank piece of paper or blank window in a mind mapping 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.tonybuzan.com.

For example, Figure I-4 shows a sample mind map that begins to output some of the IPv6 content from Part VIII of the ICND1 book. You might create this kind of mind map when reviewing IPv6 addressing concepts, starting with the big topic of "IPv6 addressing," and then writing down random terms and ideas. As you start to organize them mentally, you draw lines connecting the ideas, reorganize them, and eventually reach the point where you believe the organization of ideas makes sense to you.

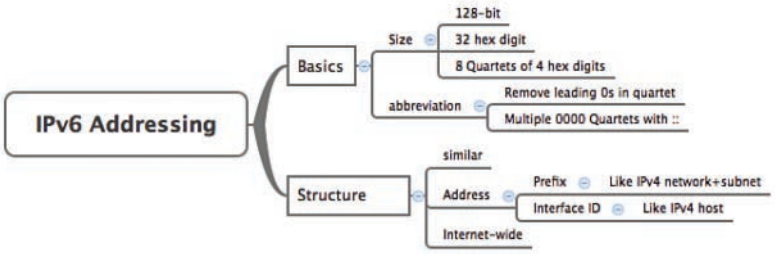


Figure I-4 *Sample Mind Map*

Mind maps may be the least popular but most effective study tool suggested in this book. I personally find a huge improvement in learning new areas of study when I mind map; I hope you will make the effort to try these tools and see if they work well for you too.

Finally, for mind mapping tools, you can just draw them on a blank piece of paper, or find and download a mind map application. I have used Mind Node Pro on a Mac, and we build the sample mind maps with XMIND, which has free versions for Windows, Linux, and OS X.

About Building Hands-On Skills

You need skills in using Cisco routers and switches, specifically the Cisco 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.

This section walks through the options included in the book, with a brief description of lab options outside the book.

Config Lab Exercises

Some router and switch features require multiple configuration commands. Part of the skill you need to acquire is the ability to remember which configuration commands work together, which ones are required, and which ones are optional. So, the challenge level goes beyond just picking the right parameters on one command. You have to choose which commands to use, in which combination, typically on multiple devices. And getting good at that kind of task requires practice.

The Config Labs feature, introduced as a new feature in this edition of the book, helps provide that practice. Each lab presents a sample lab topology, with some requirements, and you have to decide what to configure on each device. The answer then shows a sample configuration. You job is to create the configuration, and then check your answer versus the supplied answer.

Also for the first time, this edition places the content not only outside the book but also on the author's blog site. To reach my blog sites for ICND1 content or for ICND2 content (two different blogs) and access the Config Labs feature, you can start at my blog launch site (blog.certskills.com) and click from there.

blog.certskills.com/ccent/ Wendell's CCENT (ICND1): In the menus, navigate to **Hands On > Config Lab**

blog.certskills.com/ccna/ Wendell's CCNA (ICND2): In the menus, navigate to **Hands On > Config Lab**

Both blogs are geared toward helping you pass the exams, so feel free to look around. Note that the Config Lab posts should show an image like this in the summary:

Figure I-5 *Config Lab Logo in the Author's Blogs*

These Config Labs have several benefits, including the following:

- **Untethered and responsive:** Do them from anywhere, from any web browser, from your phone or tablet, untethered from the book or DVD.
- **Designed for idle moments:** Each lab is designed as a 5- to 10-minute exercise if all you are doing is typing in a text editor or writing your answer on paper.
- **Two outcomes, both good:** Practice getting better and faster with basic configuration, or if you get lost, you have discovered a topic that you can now go back and reread to complete your knowledge. Either way, you are a step closer to being ready for the exam!
- **Blog format:** Allows easy adds and changes by me, and easy comments by you.
- **Self-assessment:** As part of final review, you should be able to do all the Config Labs, without help, and with confidence.

Note that the blog organizes these Config Lab posts by book chapter, so you can easily use these at both Chapter Review and Part Review. See the "Your Study Plan" element that follows the Introduction for more details about those review sections.

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 is that you have a free and simple first step to experience the CLI: Install and use the Pearson NetSim Lite that comes with this book.

This book comes with a lite version of the best-selling CCNA Network Simulator from Pearson, which 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 NetSim Lite from the DVD in the back of this book.

The latest version of NetSim Lite includes labs associated with Part II of this book. Part I includes concepts only, with Part II being the first part with commands. So, make sure and use NetSim Lite to learn the basics of the CLI to get a good start.

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.

The Pearson Network Simulator

The Config Labs and the Pearson Network Simulator Lite both fill specific needs, and they both come with the book. However, you need more than those two tools.

The single best option for lab work to do along with this book is the paid version of the Pearson Network Simulator. This simulator product simulates Cisco routers and switches so that you can learn for the CCENT and CCNA R&S certifications. But more importantly, it focuses on learning for the exam by providing a large number of useful lab exercises. Reader surveys tell us that those people who use the Simulator along with the book love the learning process, and rave about how the book and Simulator work well together.

Of course, you need to make a decision for yourself, and consider all the options. Thankfully, you can get a great idea of how the full Simulator product works by using the Pearson Network Simulator Lite product included with the book. Both have the same base code and same user interface, and the same types of labs. Try the Lite version, and check out the full product. There is a full product for CCENT only, and another for CCNA R&S (which includes all the labs in the CCENT product, plus others for the ICND2 parts of the content).

Note that the Simulator and the books work on a different release schedule. For a time in 2016, the version of the Simulator available for purchase will be the Simulator created for the previous versions of the exams (ICND1 100-101, ICND2 200-101, and CCNA 200-120). That product includes approximately 80 percent of the CLI topics in the ICND1 100-105 and ICND2 200-105 books. So during that time, the Simulator is still very useful.

On a practical note, when you want to do labs while reading a chapter or doing Part Review, the Simulator organizes the labs to match the book. Just look for the "Sort by Chapter" tab in the Simulator's user interface. However, during the months in 2016 for which the available Simulator is the older edition listing the older exams in the title, you will need to refer back to a PDF that lists those labs versus this book's organization; find that PDF at http://www.ciscopress.com/title/9781587205798.

More Lab Options

If you decide against using the full Pearson Network Simulator, you still need hands-on experience. You should plan to use some lab environment to practice as much CLI interaction as possible.

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. If you have the right mix of gear, you could even do the Config Lab exercises from my blog on that gear, or try and re-create examples from the book.

Cisco offers a virtualization product that lets you run router and switch operating system (OS) images in a virtual environment. This tool, the Virtual Internet Routing Lab (VIRL), lets you create a lab topology, start the topology, and connect to real router and switch OS images. Check out http://virl.cisco.com for more information.

You can even rent virtual Cisco router and switch lab pods from Cisco, in an offering called Cisco Learning Labs.

All these previously mentioned options cost some money, but the next two are generally free to the user, but with a different catch for each. First, GNS3 works somewhat like VIRL, creating a virtual environment running real Cisco IOS. However, GNS3 is not a Cisco product, and cannot provide you with the IOS images for legal reasons.

Cisco also makes a simulator that works very well as a learning tool: Cisco Packet Tracer. However, Cisco intends Packet Tracer for use by people currently enrolled in Cisco Networking Academy courses, and not for the general public. So, if you are part of a Cisco Academy, definitely use Packet Tracer.

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.

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 *CCNA ICND2 200-105 Official Cert Guide* helps you attain CCNA Routing and Switching certification. This is the CCNA and 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

TCP/IP networks need IP routes. Part II collects six chapters focused on the IPv4 routing protocols discussed within the scope of ICND2.

The first four chapters in this part of the book deliver the details of OSPF Version 2 and then EIGRP. Chapter 7 begins with OSPFv2 concepts, followed by OSPFv2 implementation details (configuration and verification) in Chapter 8. Chapters 9 and 10 take the same approach to EIGRP, with one chapter of concepts (Chapter 9) and one chapter of implementation details (Chapter 10).

Chapter 11 pulls those four chapters about the OSPFv2 and EIGRP routing protocols together by discussing troubleshooting for both topics. Although they are different protocols, troubleshooting EIGRP and OSPFv2 requires the same kinds of logic and items to check. This chapter works through the details.

Finally, for the first time in the history of Cisco's CCNA R&S exam, Cisco has added more than a basic mention of BGP to the exam topics. Chapter 12 closes Part II with discussion of External BGP (eBGP), used between an enterprise and an ISP. That discussion includes basic concepts, configuration, and verification.

Part II

IPv4 Routing Protocols

Chapter 7: Understanding OSPF Concepts

Chapter 8: Implementing OSPF for IPv4

Chapter 9: Understanding EIGRP Concepts

Chapter 10: Implementing EIGRP for IPv4

Chapter 11: Troubleshooting IPv4 Routing Protocols

Chapter 12: Implementing External BGP

Part II Review

Chapter 8

Implementing OSPF for IPv4

Chapter 7, "Understanding OSPF Concepts," introduced you to the concepts, so this chapter moves on to the implementation details for Open Shortest Path First Version 2 (OSPFv2)—that is, OSPF as used for IPv4. This chapter looks at how to configure and verify a variety of OSPFv2 features.

This chapter touches on a wide variety of configuration options, so it breaks the content down into the three major sections. The first major section shows how to configure and verify basic OSPFv2 with a single-area design. With a single area, all interfaces sit in the same area, and that fact has an impact on the kinds of information lists in **show** command output. Also, the first section uses traditional OSPFv2 configuration using the OSPF **network** command. The second major section repeats the same kinds of configuration and verification as in the first major section, but now with multiarea OSPF designs.

The third major section of the chapter looks at a variety of common OSPFv2 features. These features include a completely different way to enable OSPFv2 on a Cisco router, using interface subcommands rather than the OSPF **network** command. It also includes the configuration of OSPF default routes, tuning OSPF metrics, and OSPF load balancing.

Finally, take a moment to reread the exam topics at the top of this page. Note that the exam topics specifically exclude some OSPF topics.

This chapter covers the following exam topics:

2.0 Routing Technologies

2.4 Configure, verify, and troubleshoot single area and multiarea OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

Foundation Topics

Implementing Single-Area OSPFv2

OSPF configuration includes only a few required steps, but it has many optional steps. After an OSPF design has been chosen—a task that can be complex in larger IP internetworks—the configuration can be as simple as enabling OSPF on each router interface and placing that interface in the correct OSPF area.

This section shows several configuration examples, all with a single-area OSPF internetwork. Following those examples, the text goes on to cover several of the additional optional configuration settings. For reference, the following list outlines the configuration steps covered in this first major section of the chapter, as well as a brief reference to the required commands:

Config Checklist

Step 1. Use the **router ospf** *process-id* global command to enter OSPF configuration mode for a particular OSPF process.

Step 2. (Optional) Configure the OSPF router ID by doing the following:

- **A.** Use the **router-id** *id-value* router subcommand to define the router ID
- **B.** Use the **interface loopback** *number* global command, along with an **ip address** *address mask* command, to configure an IP address on a loopback interface (chooses the highest IP address of all working loopbacks)
- **C.** Rely on an interface IP address (chooses the highest IP address of all working nonloopbacks)

Step 3. Use one or more **network** *ip-address wildcard-mask* **area** *area-id* router subcommands to enable OSPFv2 on any interfaces matched by the configured address and mask, enabling OSPF on the interface for the listed area.

Step 4. (Optional) Use the **passive-interface** *type number* router subcommand to configure any OSPF interfaces as passive if no neighbors can or should be discovered on the interface.

For a more visual perspective on OSPFv2 configuration, Figure 8-1 shows the relationship between the key OSPF configuration commands. Note that the configuration creates a routing process in one part of the configuration, and then indirectly enables OSPF on each interface. The configuration does not name the interfaces on which OSPF is enabled, instead requiring IOS to apply some logic by comparing the OSPF **network** command to the interface **ip address** commands. The upcoming example discusses more about this logic.

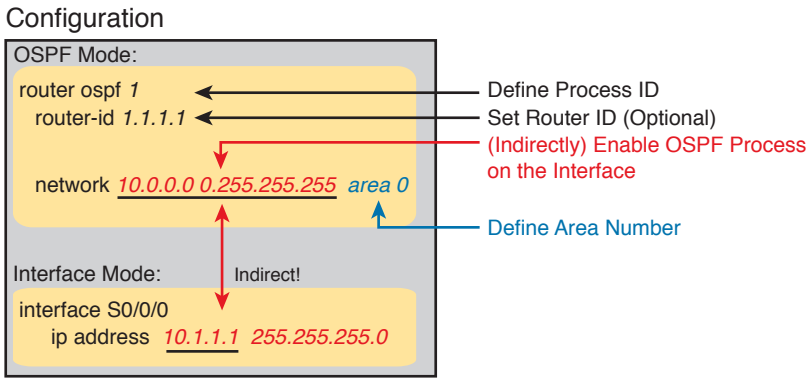


Figure 8-1 *Organization of OSPFv2 Configuration*

OSPF Single-Area Configuration

Figure 8-2 shows a sample network that will be used for the single-area OSPF configuration examples. All links sit in area 0. The design has four routers, each connected to one or two LANs. However, note that Routers R3 and R4, at the top of the figure, connect to the same two VLANs/subnets, so they will form neighbor relationships with each other over each of those VLANs as well. (The two switches at the top of the design are acting as Layer 2 switches.)

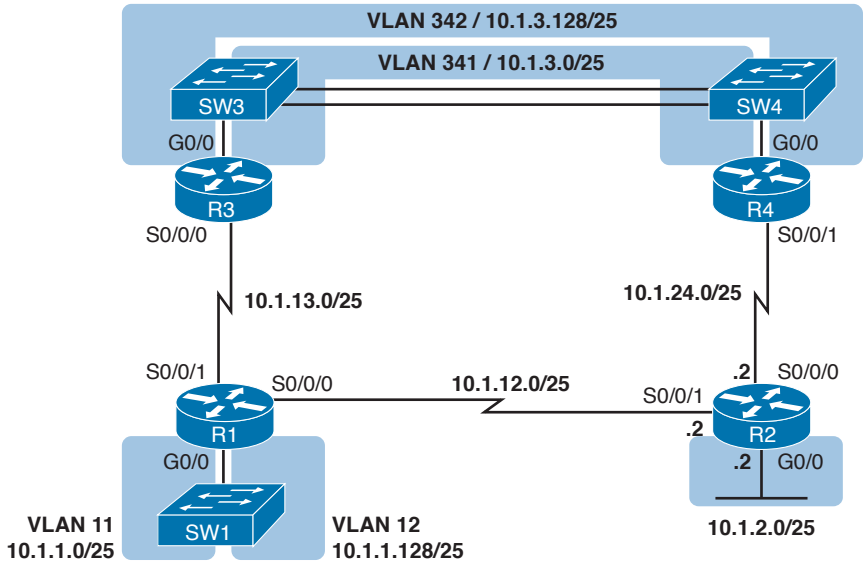


Figure 8-2 *Sample Network for OSPF Single-Area Configuration*

Example 8-1 shows the IPv4 addressing configuration on Router R3, before getting into the OSPF detail. The configuration enables 802.1Q trunking on R3's G0/0 interface, and assigns an IP address to each subinterface. (Not shown, switch S3 has configured trunking on the other side of that Ethernet link.)

Example 8-1 *IPv4 Address Configuration on R3 (Including VLAN Trunking)*

```
interface GigabitEthernet 0/0.341
 encapsulation dot1q 341
 ip address 10.1.3.1 255.255.255.128
!
interface GigabitEthernet 0/0.342
 encapsulation dot1q 342
 ip address 10.1.3.129 255.255.255.128
!
interface serial 0/0/0
 ip address 10.1.13.3 255.255.255.128
```

The beginning single-area configuration on R3, as shown in Example 8-2, enables OSPF on all the interfaces shown in Figure 8-2. First, the **router ospf 1** global command puts the user in OSPF configuration mode, and sets the OSPF *process-id*. This number just needs to be unique on the local router, allowing the router to support multiple OSPF processes in a single router by using different process IDs. (The **router** command uses the *process-id* to distinguish between the processes.) The *process-id* does not have to match on each router, and it can be any integer between 1 and 65,535.

Example 8-2 *OSPF Single-Area Configuration on R3 Using One* **network** *Command*

```
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

Speaking generally rather than about this example, the OSPF **network** command tells a router to find its local interfaces that match the first two parameters on the **network** command. Then, for each matched interface, the router enables OSPF on those interfaces, discovers neighbors, creates neighbor relationships, and assigns the interface to the area listed in the **network** command. (Note that the area can be configured as either an integer or a dotted-decimal number, but this book makes a habit of configuring the area number as an integer. The integer area numbers range from 0 through 4,294,967,295.)

For the specific command in Example 8-2, any matched interfaces are assigned to area 0. However, the first two parameters—the *ip_address* and *wildcard_mask* parameter values of 10.0.0.0 and 0.255.255.255—need some explaining. In this case, the command matches all three interfaces shown for Router R3; the next topic explains why.

Matching with the OSPF network Command

The key to understanding the traditional OSPFv2 configuration shown in this first example is to understand the OSPF **network** command. The OSPF **network** command compares the first parameter in the command to each interface IP address on the local router, trying to find a match. However, rather than comparing the entire number in the **network** command to the entire IPv4 address on the interface, the router can compare a subset of the octets, based on the wildcard mask, as follows:

Key Topic

Wildcard 0.0.0.0: Compare all 4 octets. In other words, the numbers must exactly match.

Wildcard 0.0.0.255: Compare the first 3 octets only. Ignore the last octet when comparing the numbers.

Wildcard 0.0.255.255: Compare the first 2 octets only. Ignore the last 2 octets when comparing the numbers.

Wildcard 0.255.255.255: Compare the first octet only. Ignore the last 3 octets when comparing the numbers.

Wildcard 255.255.255.255: Compare nothing—this wildcard mask means that all addresses will match the **network** command.

Basically, a wildcard mask value of 0 in an octet tells IOS to compare to see if the numbers match, and a value of 255 tells IOS to ignore that octet when comparing the numbers.

The **network** command provides many flexible options because of the wildcard mask. For example, in Router R3, many **network** commands could be used, with some matching all interfaces, and some matching a subset of interfaces. Table 8-1 shows a sampling of options, with notes.

Table 8-1 Example OSPF **network** Commands on R3, with Expected Results

Command	Logic in Command	Matched Interfaces
network 10.1.0.0 0.0.255.255	Match interface IP addresses that begin with 10.1	G0/0.341 G0/0.342 S0/0/0
network 10.0.0.0 0.255.255.255	Match interface IP addresses that begin with 10	G0/0.341 G0/0.342 S0/0/0

Command	Logic in Command	Matched Interfaces
network 0.0.0.0 255.255.255.255	Match all interface IP addresses	G0/0.341 G0/0.342 S0/0/0
network 10.1.13.0 0.0.0.255	Match interface IP addresses that begin with 10.1.13	S0/0/0
network 10.1.3.1 0.0.0.0	Match one IP address: 10.1.3.1	G0/0.341

The wildcard mask gives the local router its rules for matching its own interfaces. For example, Example 8-2 shows R3 using the **network 10.0.0.0 0.255.255.255 area 0** command. However, the wildcard mask allows for many different valid OSPF configurations. For instance, in that same internetwork, Routers R1 and R2 could use the configuration shown in Example 8-3, with two other wildcard masks. In both routers, OSPF is enabled on all the interfaces shown in Figure 8-2.

Example 8-3 *OSPF Configuration on Routers R1 and R2*

```
! R1 configuration next - one network command enables OSPF
! on all three interfaces
router ospf 1
 network 10.1.0.0 0.0.255.255 area 0
```

```
! R2 configuration next - One network command per interface
router ospf 1
 network 10.1.12.2 0.0.0.0 area 0
 network 10.1.24.2 0.0.0.0 area 0
 network 10.1.2.2 0.0.0.0 area 0
```

Finally, note that other wildcard mask values can be used as well, as long as the wildcard mask in binary is one unbroken string of 0s and another single string of binary 1s. Basically, that includes all wildcard masks that could be used to match all IP addresses in a subnet, as discussed in the "Finding the Right Wildcard Mask to Match a Subnet" section of Chapter 16, "Basic IPv4 Access Control Lists" (which is Chapter 25 of the ICND1 Cert Guide). For example, a mask of 0.255.255.0 would not be allowed.

NOTE The first two parameters of the **network** command are the address and the wildcard mask. By convention, if the wildcard mask octet is 255, the matching address octet should be configured as a 0. Interestingly, IOS will actually accept a **network** command that breaks this rule, but then IOS will change that octet of the address to a 0 before putting it into the running configuration file. For example, IOS will change a typed command that begins with **network 1.2.3.4 0.0.255.255** to **network 1.2.0.0 0.0.255.255**.

Verifying OSPFv2 Single Area

As mentioned in Chapter 7, OSPF routers use a three-step process to eventually add OSPF-learned routes to the IP routing table. First, they create neighbor relationships. Then they build and flood LSAs, so each router in the same area has a copy of the same LSDB. Finally, each router independently computes its own IP routes using the SPF algorithm and adds them to its routing table.

The **show ip ospf neighbor**, **show ip ospf database**, and **show ip route** commands display information for each of these three steps, respectively. To verify OSPF, you can use the same sequence.

Or, you can just go look at the IP routing table, and if the routes look correct, OSPF probably worked.

For example, first, examine the list of neighbors known on Router R3 from the configuration in Examples 8-1, 8-2, and 8-3. R3 should have one neighbor relationship with R1, over the serial link. It also has two neighbor relationships with R4, over the two different VLANs to which both routers connect. Example 8-4 shows all three.

Key Topic

Example 8-4 *OSPF Neighbors on Router R3 from Figure 8-2*

```
R3# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:33    10.1.13.1       Serial0/0/0
10.1.24.4         1   FULL/DR         00:00:35    10.1.3.130      GigabitEthernet0/0.342
10.1.24.4         1   FULL/DR         00:00:36    10.1.3.4        GigabitEthernet0/0.341
```

The detail in the output mentions several important facts, and for most people, working right to left works best in this case. For example, looking at the headings:

Interface: This is the local router's interface connected to the neighbor. For example, the first neighbor in the list is reachable through R3's S0/0/0 interface.

Address: This is the neighbor's IP address on that link. Again, for this first neighbor, the neighbor, which is R1, uses IP address 10.1.13.1.

State: While many possible states exist, for the details discussed in this chapter, FULL is the correct and fully working state in this case.

Neighbor ID: This is the router ID of the neighbor.

Next, Example 8-5 shows the contents of the LSDB on Router R3. Interestingly, when OSPF is working correctly in an internetwork with a single-area design, all the routers will have the same LSDB contents. So, the **show ip ospf database** command in Example 8-5 should list the same exact information, no matter on which of the four routers it is issued.

Example 8-5 *OSPF Database on Router R3 from Figure 8-2*

```
R3# show ip ospf database

            OSPF Router with ID (10.1.13.3) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         498         0x80000006 0x002294 6
2.2.2.2         2.2.2.2         497         0x80000004 0x00E8C6 5
10.1.13.3       10.1.13.3       450         0x80000003 0x001043 4
10.1.24.4       10.1.24.4       451         0x80000003 0x009D7E 4

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.3.4        10.1.24.4       451         0x80000001 0x0045F8
10.1.3.130      10.1.24.4       451         0x80000001 0x00546B
```

For the purposes of this book, do not be concerned about the specifics in the output of this command. However, for perspective, note that the LSDB should list one "Router Link State" (Type 1 Router LSA) for each of the routers in the same area. In this design, all four routers are in the same area, so there are four highlighted Type 1 LSAs listed.

Next, Example 8-6 shows R3's IPv4 routing table with the **show ip route** command. Note that it lists connected routes as well as OSPF routes. Take a moment to look back at Figure 8-2, and look for the subnets that are not locally connected to R3. Then look for those routes in the output in Example 8-5.

Example 8-6 *IPv4 Routes Added by OSPF on Router R3 from Figure 8-2*

```
R3# show ip route
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
! Legend lines omitted for brevity



      10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
O        10.1.1.0/25 [110/65] via 10.1.13.1, 00:13:28, Serial0/0/0
O        10.1.1.128/25 [110/65] via 10.1.13.1, 00:13:28, Serial0/0/0
O        10.1.2.0/25 [110/66] via 10.1.3.130, 00:12:41, GigabitEthernet0/0.342
                     [110/66] via 10.1.3.4, 00:12:41, GigabitEthernet0/0.341
C        10.1.3.0/25 is directly connected, GigabitEthernet0/0.341
L        10.1.3.1/32 is directly connected, GigabitEthernet0/0.341
C        10.1.3.128/25 is directly connected, GigabitEthernet0/0.342
L        10.1.3.129/32 is directly connected, GigabitEthernet0/0.342
O        10.1.12.0/25 [110/128] via 10.1.13.1, 00:13:28, Serial0/0/0
C        10.1.13.0/25 is directly connected, Serial0/0/0
L        10.1.13.3/32 is directly connected, Serial0/0/0
O        10.1.24.0/25
           [110/65] via 10.1.3.130, 00:12:41, GigabitEthernet0/0.342
           [110/65] via 10.1.3.4, 00:12:41, GigabitEthernet0/0.341
```

First, take a look at the bigger ideas confirmed by this output. The code of "O" on the left identifies a route as being learned by OSPF. The output lists five such IP routes. From Figure 8-2, five subnets exist that are not connected subnets off Router R3. Looking for a quick count of OSPF routes, versus nonconnected routes in the diagram, gives a quick check of whether OSPF learned all routes.

Next, take a look at the first route (to subnet 10.1.1.0/25). It lists the subnet ID and mask, identifying the subnet. It also lists two numbers in brackets. The first, 110, is the administrative distance of the route. All the OSPF routes in this example use the default of 110. The second number, 65, is the OSPF metric for this route.

Additionally, the **show ip protocols** command is also popular as a quick look at how any routing protocol works. This command lists a group of messages for each IPv4 routing protocol running on a router. Example 8-7 shows a sample, this time taken from Router R3.

Example 8-7 *The* **show ip protocols** *Command on R3*

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.13.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      06:26:17
    2.2.2.2              110      06:25:30
    10.1.24.4            110      06:25:30
  Distance: (default is 110)
```

The output shows several interesting facts. The first highlighted line repeats the parameters on the **router ospf 1** global configuration command. The second highlighted item points out R3's router ID, as discussed further in the next section. The third highlighted line repeats more configuration, listing the parameters of the **network 10.0.0.0 0.255.255.255 area 0** OSPF subcommand. Finally, the last highlighted item in the example acts as a heading before a list of known OSPF routers, by router ID.

8

Configuring the OSPF Router ID

While OSPF has many other optional features, most enterprise networks that use OSPF choose to configure each router's OSPF router ID. OSPF-speaking routers must have a router ID (RID) for proper operation. By default, routers will choose an interface IP address to use as the RID. However, many network engineers prefer to choose each router's router ID, so command output from commands like **show ip ospf neighbor** lists more recognizable router IDs.

To choose its RID, a Cisco router uses the following process when the router reloads and brings up the OSPF process. Note that when one of these steps identifies the RID, the process stops.

Key Topic

1. If the **router-id** *rid* OSPF subcommand is configured, this value is used as the RID.
2. If any loopback interfaces have an IP address configured, and the interface has an interface status of up, the router picks the highest numeric IP address among these loopback interfaces.
3. The router picks the highest numeric IP address from all other interfaces whose interface status code (first status code) is up. (In other words, an interface in up/down state will be included by OSPF when choosing its router ID.)

The first and third criteria should make some sense right away: the RID is either configured or is taken from a working interface's IP address. However, this book has not yet explained the concept of a *loopback interface*, as mentioned in Step 2.

A loopback interface is a virtual interface that can be configured with the **interface loopback** *interface-number* command, where *interface-number* is an integer. Loopback interfaces are always in an "up and up" state unless administratively placed in a shutdown state. For example, a simple configuration of the command **interface loopback 0**, followed by **ip address 2.2.2.2 255.255.255.0**, would create a loopback interface and assign it an IP address. Because loopback interfaces do not

rely on any hardware, these interfaces can be up/up whenever IOS is running, making them good interfaces on which to base an OSPF RID.

Example 8-8 shows the configuration that existed in Routers R1 and R2 before the creation of the **show** command output in Examples 8-4, 8-5, and 8-6. R1 set its router ID using the direct method, while R2 used a loopback IP address.

Example 8-8 *OSPF Router ID Configuration Examples*

```
! R1 Configuration first
router ospf 1
 router-id 1.1.1.1
 network 10.1.0.0 0.0.255.255 area 0
```

```
! R2 Configuration next
!
interface Loopback2
 ip address 2.2.2.2 255.255.255.255
```

Each router chooses its OSPF RID when OSPF is initialized, which happens when the router boots or when a CLI user stops and restarts the OSPF process (with the **clear ip ospf process** command). So, if OSPF comes up, and later the configuration changes in a way that would impact the OSPF RID, OSPF does not change the RID immediately. Instead, IOS waits until the next time the OSPF process is restarted.

Example 8-9 shows the output of the **show ip ospf** command on R1, after the configuration of Example 8-8 was made, and after the router was reloaded, which made the OSPF router ID change.

Example 8-9 *Confirming the Current OSPF Router ID*

```
R1# show ip ospf
 Routing Process "ospf 1" with ID 1.1.1.1
! lines omitted for brevity
```

OSPF Passive Interfaces

Once OSPF has been enabled on an interface, the router tries to discover neighboring OSPF routers and form a neighbor relationship. To do so, the router sends OSPF Hello messages on a regular time interval (called the Hello Interval). The router also listens for incoming Hello messages from potential neighbors.

Sometimes, a router does not need to form neighbor relationships with neighbors on an interface. Often, no other routers exist on a particular link, so the router has no need to keep sending those repetitive OSPF Hello messages.

When a router does not need to discover neighbors off some interface, the engineer has a couple of configuration options. First, by doing nothing, the router keeps sending the messages, wasting some small bit of CPU cycles and effort. Alternately, the engineer can configure the interface as an OSPF passive interface, telling the router to do the following:

Key Topic

- Quit sending OSPF Hellos on the interface.
- Ignore received Hellos on the interface.
- Do not form neighbor relationships over the interface.

By making an interface passive, OSPF does not form neighbor relationships over the interface, but it does still advertise about the subnet connected to that interface. That is, the OSPF configuration enables OSPF on the interface (using the **network** router subcommand), and then makes the interface passive (using the **passive-interface** router subcommand).

To configure an interface as passive, two options exist. First, you can add the following command to the configuration of the OSPF process, in router configuration mode:

passive-interface *type number*

Alternately, the configuration can change the default setting so that all interfaces are passive by default, and then add a **no passive-interface** command for all interfaces that need to not be passive:

passive-interface default

no passive interface *type number*

For example, in the sample internetwork in Figure 8-2 (used in the single-area configuration examples), Router R1, at the bottom left of the figure, has a LAN interface configured for VLAN trunking. The only router connected to both VLANs is Router R1, so R1 will never discover an OSPF neighbor on these subnets. Example 8-10 shows two alternative configurations to make the two LAN subinterfaces passive to OSPF.

Example 8-10 *Configuring Passive Interfaces on R1 and R2 from Figure 8-2*

```
! First, make each subinterface passive directly
router ospf 1
 passive-interface GigabitEthernet0/0.11
 passive-interface GigabitEthernet0/0.12

! Or, change the default to passive, and make the other interfaces
! not be passive

router ospf 1
 passive-interface default
 no passive-interface serial0/0/0
 no passive-interface serial0/0/1
```

In real internetworks, the choice of configuration style reduces to which option requires the least number of commands. For example, a router with 20 interfaces, 18 of which are passive to OSPF, has far fewer configuration commands when using the **passive-interface default** command to change the default to passive. If only two of those 20 interfaces need to be passive, use the default setting, in which all interfaces are not passive, to keep the configuration shorter.

Interestingly, OSPF makes it a bit of a challenge to use **show** commands to find whether or not an interface is passive. The **show running-config** command lists the configuration directly, but if you cannot get into enable mode to use this command, note these two facts:

The **show ip ospf interface brief** command lists all interfaces on which OSPF is enabled, *including passive interfaces*.

The **show ip ospf interface** command lists a single line that mentions that the interface is passive.

Example 8-11 shows these two commands on Router R1, with the configuration shown in the top of Example 8-10. Note that subinterfaces G0/0.11 and G0/0.12 both show up in the output of **show ip ospf interface brief**.

Example 8-11 *Displaying Passive Interfaces*

```
R1# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Gi0/0.12     1     0               10.1.1.129/25      1     DR    0/0
Gi0/0.11     1     0               10.1.1.1/25        1     DR    0/0
Se0/0/0      1     0               10.1.12.1/25       64    P2P   0/0
Se0/0/1      1     0               10.1.13.1/25       64    P2P   0/0

R1# show ip ospf interface g0/0.11
GigabitEthernet0/0.11 is up, line protocol is up
  Internet Address 10.1.1.1/25, Area 0, Attached via Network Statement
  Process ID 1, Router ID 10.1.1.129, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.129, Interface address 10.1.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
! Lines omitted for brevity
```

Implementing Multiarea OSPFv2

Configuring the routers in a multiarea design is almost just like configuring OSPFv2 for a single area. The only difference is that the configuration places some interfaces on each ABR in different areas. The differences come in the verification and operation of OSPFv2.

This second major section of the chapter provides a second set of configurations to contrast multiarea configuration with single-area configuration. This new scenario shows the configuration for the routers in the multiarea OSPF design based on Figures 8-3 and 8-4. Figure 8-3 shows the internetwork topology and subnet IDs, and Figure 8-4 shows the area design. Note that Figure 8-3 lists the last octet of each router's IPv4 address near each interface, rather than the entire IPv4 address, to reduce clutter.

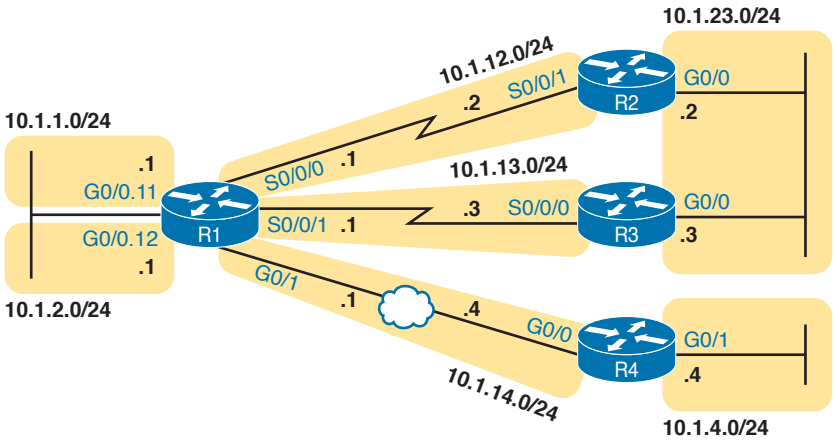


Figure 8-3 *Subnets for a Multiarea OSPF Configuration Example*

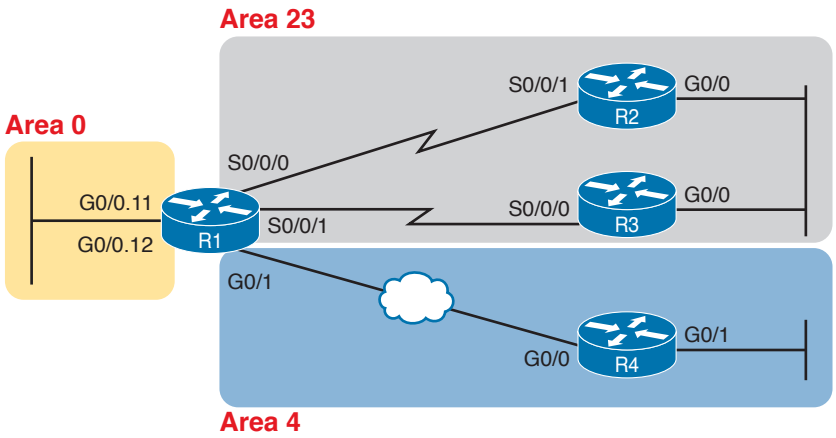


Figure 8-4 *Area Design for an Example Multiarea OSPF Configuration*

Take a moment to think about the area design shown in Figure 8-4, and look for the ABRs. Only R1 connects to the backbone area at all. The other three routers are internal routers in a single area. So, as it turns out, three of the four routers have single-area configurations, with all interfaces in the same area.

Note that the examples in this section use a variety of configuration options just so you can see those options. The options include different ways to set the OSPF RID, different wildcard masks on OSPF **network** commands, and the use of passive interfaces where no other OSPF routers should exist off an interface.

8

Single-Area Configurations

Example 8-12 begins the configuration example by showing the OSPF and IP address configuration on R2. Note that R2 acts as an internal router in area 23, meaning that the configuration will refer to only one area (23). The configuration sets R2's RID to 2.2.2.2 directly with the **router-id** command. And, because R2 should find neighbors on both its two interfaces, neither can reasonably be made passive, so R2's configuration lists no passive interfaces.

Example 8-12 *OSPF Configuration on R2, Placing Two Interfaces into Area 23*

```
interface GigabitEthernet0/0
 ip address 10.1.23.2 255.255.255.0
!
interface serial 0/0/1
 ip address 10.1.12.2 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 23
 router-id 2.2.2.2
```

Example 8-13 continues reviewing a few commands with the configuration for both R3 and R4. R3 puts both its interfaces into area 23, per its **network** command, sets its RID to 3.3.3.3 by using a loopback interface, and, like R2, cannot make either of its interfaces passive. The R4 configuration is somewhat different, with both interfaces placed into area 4, setting its RID based on a nonloopback interface (G0/0, for OSPF RID 10.1.14.4), and making R4's G0/1 interface passive, because no other OSPF routers sit on that link. (Note that the choice to use one method over another to set the OSPF RID is simply to show the variety of configuration options.)

Example 8-13 *OSPF Single-Area Configuration on R3 and R4*

```
! First, on R3
interface GigabitEthernet0/0
 ip address 10.1.23.3 255.255.255.0
!
interface serial 0/0/0
 ip address 10.1.13.3 255.255.255.0
!
interface loopback 0
 ip address 3.3.3.3 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 23
```

```
! Next, on R4
interface GigabitEthernet0/0
 description R4 will use this interface for its OSPF RID
 ip address 10.1.14.4 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 10.1.4.4 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 4
 passive-interface GigabitEthernet0/1
```

Multiarea Configuration

The only router that has a multiarea config is an ABR, by virtue of the configuration referring to more than one area. In this design (as shown in Figure 8-4), only Router R1 acts as an ABR, with interfaces in three different areas. Example 8-14 shows R1's OSPF configuration. Note that the configuration does not state anything about R1 being an ABR; instead, it uses multiple **network** commands, some placing interfaces into area 0, some into area 23, and some into area 4.

Key Topic

Example 8-14 *OSPF Multiarea Configuration on Router R1*

```
interface GigabitEthernet0/0.11
 encapsulation dot1q 11
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/0.12
 encapsulation dot1q 12
 ip address 10.1.2.1 255.255.255.0
!
```

```
interface GigabitEthernet0/1
 ip address 10.1.14.1 255.255.255.0
!
interface serial 0/0/0
 ip address 10.1.12.1 255.255.255.0
!
interface serial 0/0/1
 ip address 10.1.13.1 255.255.255.0
!
router ospf 1
 network 10.1.1.1 0.0.0.0 area 0
 network 10.1.2.1 0.0.0.0 area 0
 network 10.1.12.1 0.0.0.0 area 23
 network 10.1.13.1 0.0.0.0 area 23
 network 10.1.14.1 0.0.0.0 area 4
 router-id 1.1.1.1
 passive-interface GigabitEthernet0/0.11
 passive-interface GigabitEthernet0/0.12
```

Focus on the highlighted **network** commands in the example. All five commands happen to use a wildcard mask of 0.0.0.0, so that each command requires a specific match of the listed IP address. If you compare these **network** commands to the various interfaces on Router R1, you can see that the configuration enables OSPF, for area 0, on subinterfaces G0/0.11 and G0/0.12, area 23 for the two serial interfaces, and area 4 for R1's G0/1 interface.

NOTE Many networks make a habit of using a 0.0.0.0 wildcard mask on OSPF **network** commands, requiring an exact match of each interface IP address, as shown in Example 8-14. This style of configuration makes it more obvious exactly which interfaces match which **network** command.

Finally, note that R1's configuration also sets its RID directly and makes its two LAN subinterfaces passive.

So, what's the big difference between single-area and multiarea OSPF configuration? Practically nothing. The only difference is that with multiarea, the ABR's **network** commands list different areas.

Verifying the Multiarea Configuration

The next few pages look at how to verify a few of the new OSPF features introduced in this chapter. Figure 8-5 summarizes the most important OSPF verification commands for reference.

This section looks at the following topics:

- Verifying the ABR interfaces are in the correct (multiple) areas
- Finding which router is DR and BDR on multiaccess links
- A brief look at the LSDB
- Displaying IPv4 routes

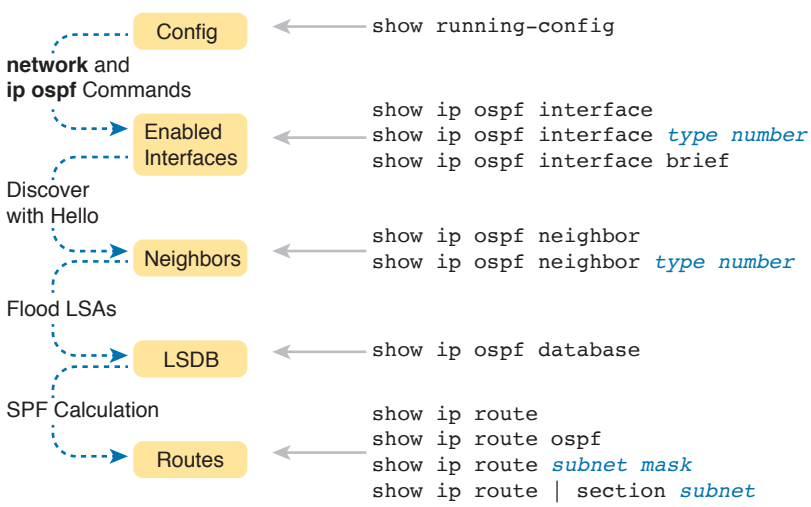


Figure 8-5 *OSPF Verification Commands*

Verifying the Correct Areas on Each Interface on an ABR

The easiest place to make a configuration oversight with a multiarea configuration is to place an interface into the wrong OSPF area. Several commands mention the OSPF area. The **show ip protocols** command basically relists the OSPF **network** configuration commands, which indirectly identify the interfaces and areas. Also, the **show ip ospf interface** and **show ip ospf interface brief** commands directly show the area configured for an interface; Example 8-15 shows an example of the briefer version of these commands.

Example 8-15 *Listing the OSPF-Enabled Interfaces and the Matching OSPF Areas*

```
R1# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Gi0/0.12     1     0               10.1.2.1/24        1     DR    0/0
Gi0/0.11     1     0               10.1.1.1/24        1     DR    0/0
Gi0/1        1     4               10.1.14.1/24       1     BDR   1/1
Se0/0/1      1     23              10.1.13.1/24       64    P2P   1/1
Se0/0/0      1     23              10.1.12.1/24       64    P2P   1/1
```

In the output, to correlate the areas, just look at the interface in the first column and the area in the third column. Also, for this example, double-check this information with Figures 8-3 and 8-4 to confirm that the configuration matches the design.

Verifying Which Router Is DR and BDR

Several **show** commands identify the DR and BDR in some way, as well. In fact, the **show ip ospf interface brief** command output, just listed in Example 8-15, lists the local router's state, showing that R1 is DR on two subinterfaces and BDR on its G0/1 interface.

Example 8-16 shows two other examples that identify the DR and BDR, but with a twist. The **show ip ospf interface** command lists detailed output about OSPF settings, per interface. Those details include the RID and interface address of the DR and BDR. At the same time, the **show ip ospf neighbor** command lists shorthand information about the neighbor's DR or BDR role as well; this command does not say anything about the local router's role.

Example 8-16 *Discovering the DR and BDR on the R1–R4 Ethernet (from R4)*

```
R4# show ip ospf interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.1.14.4/24, Area 4, Attached via Network Statement
  Process ID 1, Router ID 10.1.14.4, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.14.4, Interface address 10.1.14.4
  Backup Designated router (ID) 1.1.1.1, Interface address 10.1.14.1
!
! Lines omitted for brevity
R4# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:33    10.1.14.1       GigabitEthernet0/0
```

First, focus on the highlighted lines from the **show ip ospf interface** command output. It lists the DR as RID 10.1.14.4, which is R4. It also lists the BDR as 1.1.1.1, which is R1.

The end of the example shows the **show ip ospf neighbor** command on R4, listing R4's single neighbor, with Neighbor RID 1.1.1.1 (R1). The command lists R4's concept of its neighbor state with neighbor 1.1.1.1 (R1), with the current state listed as FULL/BDR. The FULL state means that R4 has fully exchanged its LSDB with R1. BDR means that the neighbor (R1) is acting as the BDR, implying that R4 (the only other router on this link) is acting as the DR.

Example 8-16 also shows the results of an DR/BDR election, with the router using the higher RID winning the election. The rules work like this:

- When a link comes up, if two (or more) routers on the subnet send and hear each other's Hello messages, they elect a DR and BDR, with the higher OSPF RID becoming DR, and the second highest RID becoming the BDR.
- Once the election has completed, new routers entering the subnet do not take over the DR or BDR role, even if they have better (higher) RID.

In this case, Routers R1 and R4, on the same Ethernet, heard each other's Hellos. R1, with RID 1.1.1.1, has a lower-value RID than R4's 10.1.14.1. As a result, R4 (10.1.14.1) won the DR election.

Verifying Interarea OSPF Routes

Finally, all this OSPF theory and all the **show** commands do not matter if the routers do not learn IPv4 routes. To verify the routes, Example 8-17 shows R4's IPv4 routing table.

Example 8-17 *Verifying OSPF Routes on Router R4*

```
R4# show ip route
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
```

```
      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O IA     10.1.1.0/24 [110/2] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
O IA     10.1.2.0/24 [110/2] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
C        10.1.4.0/24 is directly connected, GigabitEthernet0/1
L        10.1.4.4/32 is directly connected, GigabitEthernet0/1
O IA     10.1.12.0/24 [110/65] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
O IA     10.1.13.0/24 [110/65] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
C        10.1.14.0/24 is directly connected, GigabitEthernet0/0
L        10.1.14.4/32 is directly connected, GigabitEthernet0/0
O IA     10.1.23.0/24 [110/66] via 10.1.14.1, 11:04:43, GigabitEthernet0/0
```

This example shows a couple of new codes that are particularly interesting for OSPF. As usual, a single character on the left identifies the source of the route, with O meaning OSPF. In addition, IOS notes any interarea routes with an IA code as well. (The example does not list any intra-area OSPF routes, but these routes would simply omit the IA code; earlier Example 8-6 lists some intra-area OSPF routes.) Also, note that R4 has routes to all seven subnets in the topology used in this example: two connected routes and five interarea OSPF routes.

Additional OSPF Features

So far this chapter has focused on the most common OSPF features using the traditional configuration using the OSPF **network** command. This final of three major sections discusses some very popular but optional OSPFv2 configuration features, as listed here in their order of appearance:

- Default routes
- Metrics
- Load balancing
- OSPF interface configuration

OSPF Default Routes

In some cases, routers benefit from using a default route. The ICND1 Cert Guide showed many of the details, with the configuration of static default routes in Chapter 18, learning default routes with DHCP in Chapter 20, and advertising default routes with RIP in Chapter 19. For those exact same reasons, networks that happen to use OSPFv2 can use OSPF to advertise default routes.

The most classic case for using a routing protocol to advertise a default route has to do with an enterprise's connection to the Internet. As a strategy, the enterprise engineer uses these design goals:

- All routers learn specific routes for subnets inside the company; a default route is not needed when forwarding packets to these destinations.
- One router connects to the Internet, and it has a default route that points toward the Internet.
- All routers should dynamically learn a default route, used for all traffic going to the Internet, so that all packets destined to locations in the Internet go to the one router connected to the Internet.

Figure 8-6 shows the idea of how OSPF advertises the default route, with the specific OSPF configuration. In this case, a company connects to an ISP with its Router R1. That router has a static default route (destination 0.0.0.0, mask 0.0.0.0) with a next-hop address of the ISP router. Then, the use of the OSPF **default-information originate** command (Step 2) makes the router advertise a default route using OSPF to the remote routers (B1 and B2).

NOTE The example in Figure 8-6 uses a static default route, but it could have used a default route as learned from the ISP with DHCP, as well as learning a default route with External BGP (eBGP), as discussed in Chapter 12, "Implementing External BGP."

Key Topic

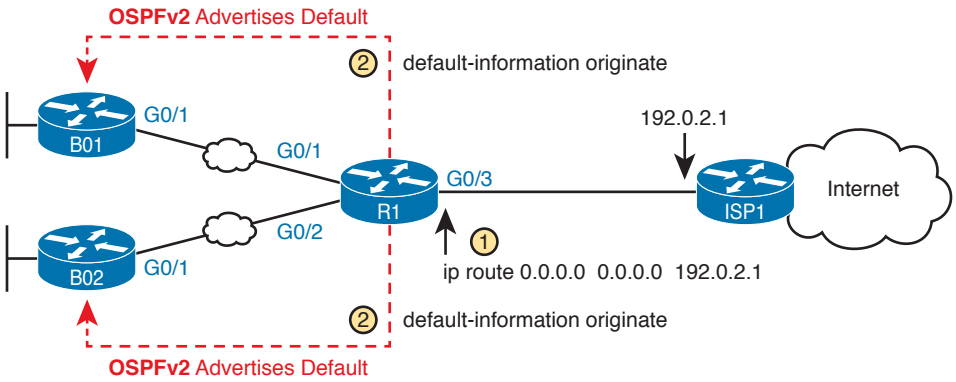


Figure 8-6 *Using OSPF to Create and Flood a Default Route*

Figure 8-7 shows the default routes that result from OSPF's advertisements in Figure 8-6. On the far left, the branch routers all have OSPF-learned default routes, pointing to R1. R1 itself also needs a default route, pointing to the ISP router, so that R1 can forward all Internet-bound traffic to the ISP.

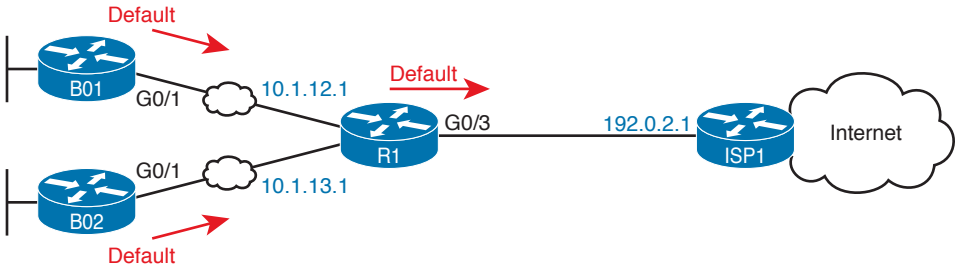


Figure 8-7 *Default Routes Resulting from the* **default-information originate** *Command*

Finally, this feature gives the engineer control over when the router originates this default route. First, R1 needs a default route, either defined as a static default route, learned from the ISP with DHCP, or learned from the ISP with a routing protocol like eBGP. The **default-information originate** command then tells R1 to advertise a default route when its own default route is working, and to advertise the default route as down when its own default route fails.

NOTE Interestingly, the **default-information originate always** router subcommand tells the router to always advertise the default route, no matter whether the router's default route is working or not.

Example 8-18 shows details of the default route on both R1 and branch router B01. Beginning with Router R1, in this case, Router R1 used DHCP to learn its IP address on its G0/3 interface from the ISP. R1 then creates a static default route with the ISP router's IP address of 192.0.2.1 as the next-hop address, as highlighted in the output of the **show ip route static** command output.

Example 8-18 *Default Routes on Routers R1 and B01*

```
! The next command is from Router R1. Note the static code for the default route
R1# show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
! Rest of the legend omitted for brevity

Gateway of last resort is 192.0.2.1 to network 0.0.0.0

S*    0.0.0.0/0 [254/0] via 192.0.2.1
```

```
! The next command is from router B01; notice the External route code for the default
BO1# 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
! Rest of the legend omitted for brevity

Gateway of last resort is 10.1.12.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.1.12.1, 00:20:51, GigabitEthernet0/1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O        10.1.3.0/24 [110/3] via 10.1.12.1, 00:20:51, GigabitEthernet0/1
O        10.1.13.0/24 [110/2] via 10.1.12.1, 00:20:51, GigabitEthernet0/1
```

Keeping the focus on the command on Router R1, note that R1 indeed has a default route, that is, a route to 0.0.0.0/0. The "Gateway of last resort," which refers to the default route currently used by the router, points to next-hop IP address 192.0.2.1, which is the ISP router's IP address. (Refer back to Figure 8-7 for the particulars.)

Next look to the bottom half of the example, and router BO1's OSPF-learned default route. BO1 lists a route for 0.0.0.0/0 as well. The next-hop router in this case is 10.1.12.1, which is Router R1's IP address on the WAN link. The code on the far left is O*E2, meaning: an OSPF-learned route, which is a default route, and is specifically an external OSPF route. Finally, BO1's gateway of last resort setting uses that one OSPF-learned default route, with next-hop router 10.1.12.1.

OSPF Metrics (Cost)

Earlier, the Chapter 7 section "Calculating the Best Routes with SPF" discussed how SPF calculates the metric for each route, choosing the route with the best metric for each destination subnet. OSPF routers can influence that choice by changing the OSPF interface cost on any and all interfaces.

Cisco routers allow two different ways to change the OSPF interface cost. The one straightforward way is to set the cost directly, with an interface subcommand: **ip ospf cost** *x*. The other method is to let IOS choose default costs, based on a formula, but to change the inputs to the formula. This second method requires a little more thought and care and is the focus of this next topic.

Setting the Cost Based on Interface Bandwidth

The default OSPF cost values can actually cause a little confusion, for a couple of reasons. So, to get through some of the potential confusion, this section begins with some examples.

First, IOS uses the following formula to choose an interface's OSPF cost. IOS puts the interface's bandwidth in the denominator, and a settable OSPF value called the *reference bandwidth* in the numerator:

Reference_bandwidth / Interface_bandwidth

With this formula, the following sequence of logic happens:

1. A higher interface bandwidth—that is, a faster bandwidth—results in a lower number in the calculation.
2. A lower number in the calculation gives the interface a lower cost.
3. An interface with a lower cost is more likely to be used by OSPF when calculating the best routes.

Now for some examples. Assume a default reference bandwidth, set to 100 Mbps, which is the same as 100,000 Kbps. (The upcoming examples will use a unit of Kbps just to avoid math with fractions.) Assume defaults for interface bandwidth on serial, Ethernet, and Fast Ethernet interfaces, as shown in the output of the **show interfaces** command, respectively, of 1544 Kbps, 10,000 Kbps (meaning 10 Mbps), and 100,000 Kbps (meaning 100 Mbps). Table 8-2 shows the results of how IOS calculates the OSPF cost for some interface examples.

Table 8-2 OSPF Cost Calculation Examples with Default Bandwidth Settings

Interface	Interface Default Bandwidth (Kbps)	Formula (Kbps)	OSPF Cost
Serial	1544 Kbps	100,000/1544	64
Ethernet	10,000 Kbps	100,000/10,000	10
Fast Ethernet	100,000 Kbps	100,000/100,000	1

Example 8-19 shows the cost settings on R1's OSPF interfaces, all based on default OSPF (reference bandwidth) and default interface bandwidth settings.

Example 8-19 *Confirming OSPF Interface Costs*

```
R1# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Gi0/0.12     1     0               10.1.2.1/24        1     DR    0/0
Gi0/0.11     1     0               10.1.1.1/24        1     DR    0/0
Gi0/1        1     4               10.1.14.1/24       1     BDR   1/1
Se0/0/1      1     23              10.1.13.1/24       64    P2P   1/1
Se0/0/0      1     23              10.1.12.1/24       64    P2P   1/1
```

To change the OSPF cost on these interfaces, the engineer simply needs to use the **bandwidth** *speed* interface subcommand to set the bandwidth on an interface. The interface bandwidth does not change the Layer 1 transmission speed at all; instead, it is used for other purposes, including routing protocol metric calculations. For instance, if you add the **bandwidth 10000** command to a serial interface, with a default reference bandwidth, the serial interface's OSPF cost could be calculated as 100,000 / 10,000 = 10.

Note that if the calculation of the default metric results in a fraction, OSPF rounds down to the nearest integer. For instance, the example shows the cost for interface S0/0/0 as 64. The calculation used the default serial interface bandwidth of 1.544 Mbps, with reference bandwidth 100 (Mbps), with the 100 / 1.544 calculation resulting in 64.7668394. OSPF rounds down to 64.

The Need for a Higher Reference Bandwidth

This default calculation works nicely as long as the fastest link in the network runs at 100 Mbps. The default reference bandwidth is set to 100, meaning 100 Mbps, the equivalent of 100,000 Kbps. As a result, with default settings, faster router interfaces end up with the same OSPF cost, as shown in Table 8-3, because the lowest allowed OSPF cost is 1.

Table 8-3 Faster Interfaces with Equal OSPF Costs

Interface	Interface Default Bandwidth (Kbps)	Formula (Kbps)	OSPF Cost
Fast Ethernet	100,000 Kbps	100,000/100,000	1
Gigabit Ethernet	1,000,000 Kbps	100,000/1,000,000	1
10 Gigabit Ethernet	10,000,000 Kbps	100,000/10,000,000	1
100 Gigabit Ethernet	100,000,000 Kbps	100,000/100,000,000	1

To avoid this issue, and change the default cost calculation, you can change the reference bandwidth with the **auto-cost reference-bandwidth** *speed* OSPF mode subcommand. This command sets a value in a unit of megabits per second (Mbps). To avoid the issue shown in Table 8-3, set the reference bandwidth value to match the fastest link speed in the network. For instance, **auto-cost reference-bandwidth 10000** accommodates links up to 10 Gbps in speed.

NOTE Cisco recommends making the OSPF reference bandwidth setting the same on all OSPF routers in an enterprise network.

For convenient study, the following list summarizes the rules for how a router sets its OSPF interface costs:

Key Topic

1. Set the cost explicitly, using the **ip ospf cost** *x* interface subcommand, to a value between 1 and 65,535, inclusive.
2. Change the interface bandwidth with the **bandwidth** *speed* command, with *speed* being a number in kilobits per second (Kbps).
3. Change the reference bandwidth, using router OSPF subcommand **auto-cost reference-bandwidth** *ref-bw*, with a unit of megabits per second (Mbps).

OSPF Load Balancing

When a router uses SPF to calculate the metric for each of several routes to reach one subnet, one route may have the lowest metric, so OSPF puts that route in the routing table. However, when the metrics tie for multiple routes to the same subnet, the router can put multiple equal-cost routes in the routing table (the default is four different routes) based on the setting of the **maximum-paths** *number* router subcommand. For example, if an internetwork has six possible paths between some parts of the network, and the engineer wants all routes to be used, the routers can be configured with the **maximum-paths 6** subcommand under **router ospf**.

The more challenging concept relates to how the routers use those multiple routes. A router could load balance the packets on a per-packet basis. For example, if the router has three equal-cost OSPF routes for the same subnet in the routing table, the router could send the one packet over the first route, the next packet over the second route, the next packet over the third route, and then start over with the first route for the next packet. Alternatively, the load balancing could be on a per-destination IP address basis.

Note that the default setting of **maximum-paths** varies by router platform.

OSPFv2 Interface Configuration

The newer interface-style OSPF configuration works mostly like the old style, for almost all features, with one important exception. The interface configuration enables OSPF directly on the interface with the **ip ospf** interface subcommand, while the traditional OSPFv2 configuration enables OSPFv2 on an interface, but indirectly, using the **network** command in OSPF configuration mode. The rest of the OSPF features discussed throughout this chapter are not changed by the use of OSPFv2 interface configuration.

Basically, instead of matching interfaces with indirect logic using **network** commands, you directly enable OSPFv2 on interfaces by configuring an interface subcommand on each interface.

OSPFv2 Interface Configuration Example

To show how OSPF interface configuration works, this example basically repeats the example shown earlier in the book using the traditional OSPFv2 configuration with **network** commands. So, before looking at the OSPFv2 interface configuration, take a moment to look back at Figures 8-3 and 8-4, along with Examples 8-12, 8-13, and 8-14. Once reviewed, for easier reference, Figure 8-8 repeats Figure 8-4 for reference in the upcoming interface configuration examples.

To convert from the old-style configuration in Examples 8-12, 8-13, and 8-14, simply do the following:

Config Checklist

Step 1. Use the **no network** *network-id* **area** *area-id* subcommands in OSPF configuration mode to remove the **network** commands.

Step 2. Add one **ip ospf** *process-id* **area** *area-id* command in interface configuration mode under each interface on which OSPF should operate, with the correct OSPF process (*process-id*) and the correct OSPF area number.

For example, Example 8-12 had a single **network** command that enabled OSPF on two interfaces on Router R2, putting both in area 23. Example 8-20 shows the replacement newer style of configuration.

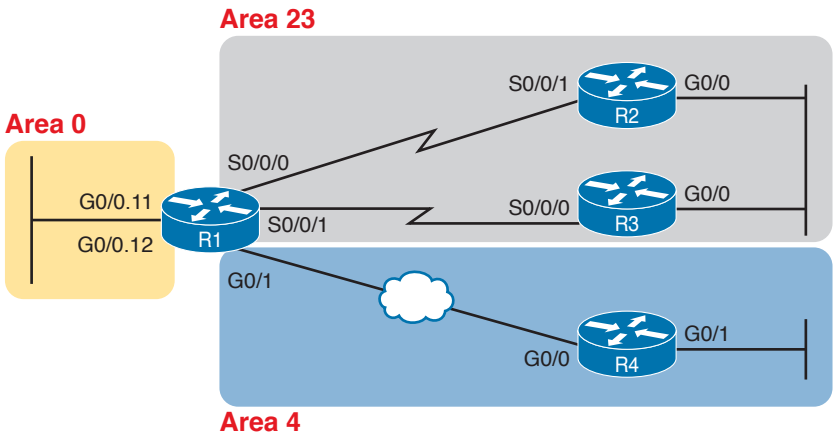


Figure 8-8 *Area Design Used in the Upcoming OSPF Example*

Example 8-20 *New-Style Configuration on Router R2*

```
interface GigabitEthernet0/0
 ip address 10.1.23.2 255.255.255.0
 ip ospf 1 area 23
!
```

```
interface serial 0/0/1
 ip address 10.1.12.2 255.255.255.0
 ip ospf 1 area 23

router ospf 1
 router-id 2.2.2.2
! Notice - no network commands here!
```

Verifying OSPFv2 Interface Configuration

OSPF operates the same way whether you use the new style or old style of configuration. The OSPF area design works the same, neighbor relationships form the same way, routers negotiate to become the DR and BDR the same way, and so on. However, you can see a few small differences in command output when using the newer OSPFv2 configuration if you look closely.

The **show ip protocols** command relists most of the routing protocol configuration, just in slightly different format, as shown in Example 8-21. With the newer-style configuration, the output lists the phrase "Interfaces Configured Explicitly," with the list of interfaces configured with the new **ip ospf** *process-id* **area** *area-id* commands, as highlighted in the example. With the old configuration, the output lists the contents of all the **network** commands, just leaving out the "network" word itself. Note that in the next two examples, R2 has been reconfigured to use OSPF interface configuration as shown in the previous example (Example 8-20), while Router R3 still uses the older-style **network** commands per earlier configuration Example 8-13.

Example 8-21 *Differences in* **show ip protocols** *Output: Old- and New-Style OSPFv2 Configuration*

```
R2# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 23):
    Serial0/0/1
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:04:59
    1.1.1.1              110      00:04:43
  Distance: (default is 110)
```

```
! Below, showing only the part that differs on R3:
R3# show ip protocols
! … beginning lines omitted for brevity
  Routing for Networks:
    10.0.0.0 0.255.255.255 area 23
! … ending line omitted for brevity
```

Basically, the **show ip protocols** command output differs depending on the style of configuration, either relisting the interfaces when using interface configuration or relisting the network commands if using **network** commands.

Next, the **show ip ospf interface** [*interface*] command lists details about OSPF settings for the interface(s) on which OSPF is enabled. The output also makes a subtle reference to whether that interface was enabled for OSPF with the old or new configuration style. As seen in Example 8-22, R2's new-style interface configuration results in the highlighted text, "Attached via Interface Enable," whereas R3's old-style configuration lists "Attached via Network Statement."

Key Topic

Example 8-22 *Differences in* **show ip ospf interface** *Output with OSPFv2 Interface Configuration*

```
R2# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.1.23.2/24, Area 23, Attached via Interface Enable
  Process ID 1, Router ID 22.2.2.2, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0          1        no          no             Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 10.1.23.2
  Backup Designated router (ID) 3.3.3.3, Interface address 10.1.23.3
```

```
! Showing only the part that differs on R3:
R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 10.1.23.3/24, Area 23, Attached via Network Statement
! … ending line omitted for brevity
```

Note that the briefer version of this command, the **show ip ospf interface brief** command, does not change whether the configuration uses traditional **network** commands or the alternative interface configuration with the **ip ospf** interface subcommand.

Review Activities

Chapter Summary

- The OSPF **network** command is used to match the IP addresses that are configured on the interfaces. Those that match are inserted into the OSPF process.
- The OSPF **network** command uses wildcard masks to control which bits in an octet are matched.
- The **show ip ospf neighbor** command can be used to find information about any OSPF neighborships, including the interface, the state, the neighbor's address, and the neighbor's router ID.
- To select a router ID for OSPF, a router goes through a process. When a router ID has been found, the process stops. The process is any value configured with the **router-id** command; the highest configured IPv4 address of any enabled loopback interface; and the highest configured IPv4 address of any physically up (up/up or up/down) physical interface.
- An OSPF interface configured as passive will quit sending OSPF Hello messages, will ignore any received Hello messages, and will not form any neighborships.
- The only OSPF router configured into multiple areas is an Area Border Router (ABR).
- The **show ip ospf interface** [*type number* | **brief**] command can be used to display which interfaces are enabled into the OSPF process.
- The **show ip ospf neighbor** [*type number*] command can be used to display any OSPF neighborships.
- The **show ip ospf database** command can be used to display the OSPF LSDB.
- The **show ip route** [**ospf** | *subnet mask*] command can be used to display OSPF routes in the current routing table.
- The **show ip protocols** and **show ip ospf interface** [**brief**] commands can be used to display which areas are configured on a device.
- The OSPF **default-information originate** command is used along with a configured static default route to advertise a default route into OSPF.
- OSPF uses three rules to set interface costs: setting the cost explicitly with the **ip ospf cost** *cost* command, changing the interface bandwidth with the **bandwidth** *bandwidth* command, or changing the reference bandwidth with the **auto-cost reference-bandwidth** *reference-bandwidth* command.
- The output of the **show ip protocols** and **show ip ospf interface** commands will differ depending on whether OSPF was configured with the old (**network**) or new (interface commands) configuration style.

Review Questions

1. Which of the following **network** commands, following the command **router ospf 1**, tells this router to start using OSPF on interfaces whose IP addresses are 10.1.1.1, 10.1.100.1, and 10.1.120.1?

   A. **network 10.0.0.0 255.0.0.0 area 0**

   B. **network 10.0.0.0 0.255.255.255 area 0**

   C. **network 10.0.0.1 0.0.0.255 area 0**

   D. **network 10.0.0.1 0.0.255.255 area 0**

2. Which of the following **network** commands, following the command **router ospf 1**, tells this router to start using OSPF on interfaces whose IP addresses are 10.1.1.1, 10.1.100.1, and 10.1.120.1?

   A. **network 10.1.0.0 0.0.255.255 area 0**

   B. **network 10.0.0.0 0.255.255.0 area 0**

   C. **network 10.1.1.0 0.x.1x.0 area 0**

   D. **network 10.1.1.0 255.0.0.0 area 0**

   E. **network 10.0.0.0 255.0.0.0 area 0**

3. Which of the following commands list the OSPF neighbors off interface serial 0/0? (Choose two answers.)

   A. **show ip ospf neighbor**

   B. **show ip ospf interface brief**

   C. **show ip neighbor**

   D. **show ip interface**

   E. **show ip ospf neighbor serial 0/0**

4. Routers R1, R2, and R3 are internal routers in areas 1, 2, and 3, respectively. Router R4 is an ABR connected to the backbone area (0) and to areas 1, 2, and 3. Which of the following answers describes the configuration on Router R4, which is different from the other three routers, that makes it an ABR?

   A. The **abr enable** router subcommand.

   B. The **network** router subcommands refer to a single nonbackbone area.

   C. The **network** router subcommands refer to multiple areas, including the backbone.

   D. The router has an interface in area 0, whereas an OSPF neighbor's interface sits in a different area.

5. An engineer connects to Router R1 and issues a **show ip ospf neighbor** command. The status of neighbor 2.2.2.2 lists FULL/BDR. What does the BDR mean?

   A. R1 is an Area Border Router.

   B. R1 is a backup designated router.

   C. Router 2.2.2.2 is an Area Border Router.

   D. Router 2.2.2.2 is a backup designated router.

6. An engineer migrates from a more traditional OSPFv2 configuration that uses **network** commands in OSPF configuration mode to instead use OSPFv2 interface configuration. Which of the following commands configures the area number assigned to an interface in this new configuration?

   A. The **area** command in interface configuration mode

   B. The **ip ospf** command in interface configuration mode

   C. The **router ospf** command in interface configuration mode

   D. The **network** command in interface configuration mode

7. Which of the following configuration settings on a router does not influence which IPv4 route a router chooses to add to its IPv4 routing table when using OSPFv2?

   A. **auto-cost reference-bandwidth**

   B. **delay**

   C. **bandwidth**

   D. **ip ospf cost**

Chapter Review

One key to doing well on the exams is to perform repetitive spaced review sessions. Review this chapter's material using either the tools in the book, DVD, or interactive tools for the same material found on the book's companion website. Refer to the "Your Study Plan" element for more details. Table 8-4 outlines the key review elements and where you can find them. To better track your study progress, record when you completed these activities in the second column.

Table 8-4 Chapter Review Tracking

Review Element	Review Date(s)	Resource Used:
Review key topics		Book, DVD/website
Review key terms		Book, DVD/website
Answer chapter review questions		Book, PCPT
Do labs		Blog
Review Config Checklists		Book, DVD/website
Review command tables		Book

Review All the Key Topics

Key Topic

Table 8-5 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
List	Example OSPF wildcard masks and their meaning	187
Example 8-4	Example of the **show ip ospf neighbor** command	189
List	Rules for setting the router ID	191
List	Actions IOS takes when an OSPF interface is passive	192
Example 8-14	Example of a multiarea OSPFv2 configuration	196
Figure 8-5	Popular OSPF **show** commands and their general purposes	198
Example 8-15	Example of the **show ip ospf interface brief** showing interfaces in multiple areas	198
Figure 8-6	Actions taken by the OSPF **default-information originate** command	201
List	Rules for setting OSPF interface cost	204
Example 8-22	Differences in **show ip ospf interface** output with OSPF interface configuration	207

Key Terms You Should Know

reference bandwidth, interface bandwidth, maximum paths

Command References

Tables 8-6 and 8-7 list configuration and verification commands used in this chapter. As an easy review exercise, cover the left column in a table, read the right column, and try to recall the command without looking. Then repeat the exercise, covering the right column, and try to recall what the command does.

Table 8-6 Chapter 8 Configuration Command Reference

Command	Description
router ospf *process-id*	Enters OSPF configuration mode for the listed process.
network *ip-address wildcard-mask* area *area-id*	Router subcommand that enables OSPF on interfaces matching the address/wildcard combination and sets the OSPF area.
ip ospf *process-id* **area** *area-number*	Interface subcommand to enable OSPF on the interface and to assign the interface to a specific OSPF area.
ip ospf cost *interface-cost*	Interface subcommand that sets the OSPF cost associated with the interface.
bandwidth *bandwidth*	Interface subcommand that directly sets the interface bandwidth (Kbps).
auto-cost reference-bandwidth *number*	Router subcommand that tells OSPF the numerator in the Reference_bandwidth / Interface_bandwidth formula used to calculate the OSPF cost based on the interface bandwidth.
router-id *id*	OSPF command that statically sets the router ID.
interface loopback *number*	Global command to create a loopback interface and to navigate to interface configuration mode for that interface.
maximum-paths *number-of-paths*	Router subcommand that defines the maximum number of equal-cost routes that can be added to the routing table.
passive-interface *type number*	Router subcommand that makes the interface passive to OSPF, meaning that the OSPF process will not form neighbor relationships with neighbors reachable on that interface.
passive-interface *default*	OSPF subcommand that changes the OSPF default for interfaces to be passive instead of active (not passive).
no passive-interface *type number*	OSPF subcommand that tells OSPF to be active (not passive) on that interface or subinterface.
default-information originate [**always**]	OSPF subcommand to tell OSPF to create and advertise an OSPF default route, as long as the router has some default route (or to always advertise a default, if the **always** option is configured).

Table 8-7 Chapter 8 EXEC Command Reference

Command	Description
show ip ospf	Lists information about the OSPF process running on the router, including the OSPF router ID, areas to which the router connects, and the number of interfaces in each area.
show ip ospf interface brief	Lists the interfaces on which the OSPF protocol is enabled (based on the **network** commands), including passive interfaces.
show ip ospf interface [*type number*]	Lists a long section of settings, status, and counters for OSPF operation on all interfaces, or on the listed interface, including the Hello and Dead Timers.
show ip protocols	Shows routing protocol parameters and current timer values.
show ip ospf neighbor [*type number*]	Lists brief output about neighbors, identified by neighbor router ID, including current state, with one line per neighbor; optionally, limits the output to neighbors on the listed interface.

Command	Description
show ip ospf neighbor *neighbor-ID*	Lists the same output as the **show ip ospf neighbor** detail command, but only for the listed neighbor (by neighbor RID).
show ip ospf database	Lists a summary of the LSAs in the database, with one line of output per LSA. It is organized by LSA type (first type 1, then type 2, and so on).
show ip route	Lists all IPv4 routes.
show ip route ospf	Lists routes in the routing table learned by OSPF.
show ip route *ip-address mask*	Shows a detailed description of the route for the listed subnet/mask.
clear ip ospf process	Resets the OSPF process, resetting all neighbor relationships and also causing the process to make a choice of OSPF RID.

Answers to the Review Questions:

1 B **2** A **3** A, E **4** C **5** D **6** B, **7** B

This page intentionally left blank

Index

Symbols

2-way state (neighbor relationships), 175, 594
3G wireless, 372
4G wireless, 372
802.1D STP, 51, 54
802.1Q, 16
  headers, 473-474
  trunking. *See* ROAS
802.1w RSTP
  defined, 51
  port roles, 53
  port states, 54
802.11 headers, 474

A

aaa authentication login default command, 141
aaa new-model command, 140
AAA servers
  authentication
    configuration, 140-141
    login authentication rules, 141-142
    login process, 139
    TACACS+/RADIUS protocols, 139-140
  configuring for 802.1x, 137
  defining, 141
  enabling, 140
  username/passwords, verifying, 138
aaS (as a Service), 705
ABR (Area Border Router), 179, 590
  interface OSPF areas, verifying, 198
  OSPFv2 multiarea configuration, 196-197
  OSPFv3 multiarea configuration, 590-591
access
  Internet, 369
    cable Internet, 371
    DSLs (digital subscriber lines), 370-371
    fiber, 372
    WANs, 369
    wireless WANs, 371-372
  IPv6 restrictions, 650
  public cloud services
    Internet, 707-709
    private WANs, 709-711
    VPNs, 709
  securing with IEEE 802.1x, 137-138
access-class command, 461
access control lists. *See* ACLs
Access Control Server (ACS), 139
access interfaces, 20, 105-106
access layer switches, 147-148
access links
  MetroE, 348
  MPLS, 358
access-list command, 421-423, 433, 437-439, 461
  building ACLs with, 428-429
  examples and logic explanations, 440-441
  extended numbered ACL configuration commands, 441
  keywords
    any, 423-424
    deny, 424
    log, 427
    permit, 421, 424
    tcp, 438
    upd, 438
  reverse engineering from ACL to address range, 429-430
ACI (Application Centric Infrastructure), 734-735

ACLs (access control lists), 553
ACL Analysis tool, 738-739
classification, 471
comparison of ACL types, 419
extended numbered ACLs
configuration, 441-444
matching protocol, source IP, and destination IP, 437-438
matching TCP and UDP port numbers, 438-441
overview, 437
GRE tunnel issues, 387-388
HSRP packets, blocking, 531
implementation considerations, 449-450
IPv4, 633
IPv6, 632-633
access-list commands, building, 644
blocking, 647
capabilities, 635-636
extended, 640-643
filtering ICMPv6 NDP messages, 645-648
filtering policies, 634
ICMPv6 message filtering, 635
implicit filtering ICMPv6 NDP messages, 648-649
IPv4 ACL, compared, 633
IPv6 access restrictions, 650
limitations, 636-637
logging, 636
management control, 649-650
prefix lengths, 636
problems, 580
router originated packets, 637
standard, configuring, 637-640
testing, 643
tunneled traffic matching, 636
location and direction, 417-418
matching packets, 418
named ACLs
configuration, 445-446
editing, 446-448
overview, 444-445
numbered ACLs, 448-449
overview, 417
QoS tools, compared, 469
SNMP security, 664
standard numbered ACLs
access-list command, 428-429
command syntax, 421
configuration examples, 424-427
list logic, 419-421
matching any/all addresses, 423-424
matching exact IP address, 421
matching subset of address, 421-423
overview, 419
reverse engineering from ACL to address range, 429-430
troubleshooting, 427-428
verification, 427-428
wildcard masks, 421-423
troubleshooting, 450
ACL behavior in network, 450-451
ACL interactions with router-generated packets, 455-457
commands, 451-452
common syntax mistakes, 453-454
inbound ACL filters routing protocol packets, 454-455
reversed source/destination IP address, 452-453
ACS (Access Control Server), 139
active HSRP routers, 527
address blocks. *See* prefixes
addresses
families, 585
global unicast, 563
IPv4, 186
IPv6
assigning to hosts, 565-567
connectivity, verifying, 569-572
multicast, 647
router configuration, 568
static route configuration, 568-569
unicast, 563-565

link, 294-295
link-local, 564
MAC, 43
public cloud assignment services, 717-718
source/destination, 384
unique local unicast, 563
adjacent neighbors, 175, 598
administrative distance, 168
administratively shutdown interfaces, 43
ADSL (asymmetric DSL), 370
advertising
BGP routes, 287-288
eBPG enterprise public prefixes, 291-292
subnets to ISPs, 300-301
AF (Assured Forwarding), 475-476
agents (SNMP), 661
Get/Set messages, 662
MIB, 663
NMS polling, 661
notifications, 662-663
algorithms
Dijkstra SPF, 170
DUAL (Diffusing Update Algorithm), 229-230, 613
IGP routing protocol algorithm, 165-166
SPF (Shortest Path First), 170, 176-177
STA (spanning-tree algorithm), 42
all IP addresses, matching, 423-424
alternate ports, 53-54, 83
Amazon Web Services (AWS), 705
American Registry for Internet Numbers (ARIN), 165
analyzers (network), 682-683
answering exam questions, 753-755
anti-replay (Internet VPNs), 373
any keyword, 423
any/all IP addresses, matching, 423-424
APIs (application programming interfaces), 730-731
APIC (Application Policy Infrastructure Controller), 735
APIC EM (APIC Enterprise Module), 735-737
controller, 738
Path Trace ACL Analysis tool, 738-739
Path Trace app, 738
Application Centric Infrastructure (ACI), 734-735
Application Policy Infrastructure Controller (APIC), 735
application signatures, 472
application-specific integrated circuit (ASIC), 728
architectures (SDN), 732
APIC Enterprise Module (APIC-EM), 735-737
Application Centric Infrastructure (ACI), 734-735
comparisons, 737
Open SDN, 732-733
Open SDN Controller (OSC), 734
OpenDaylight (ODL), 733-734
OpenFlow, 732
Area Border Router. *See* ABR
area design (OSPF), 179
ABR, 179, 198
areas, 178-179
backbone areas, 179
multiarea on ABR configuration, 591
super, 361
backbone routers, 179
benefits, 180
interarea routes, 179
internal routers, 179
intra-area routes, 179
mismatches, finding, 276-277
MPLS VPNs, 361-362
network size, 178
problems, 177, 268
single-area, 177
SPF workload, reducing, 179
three-area, 178
ARIN (American Registry for Internet Numbers), 165

AS (autonomous system), 164-165, 288
as a Service (-aaS), 705
ASAv (virtual ASA firewall), 715
ASIC (application-specific integrated circuit), 728
ASNs (AS numbers), 165
BGP, 288
EIGRP, 235
for IPv6, 615
neighbors, 223, 274
Assured Forwarding (AF), 475-476
asymmetric DSL (ADSL), 370
attacks
DHCP-based, 143-144
types, 142
auth keyword (snmp-server group command), 672
authentication
802.1x, 137
AAA servers
configuration examples, 140-141
login authentication rules, 141-142
login process, 139
TACACS+/RADIUS protocols, 139-140
EIGRP neighbors, 222, 273
Internet VPNs, 373
PPP, 325-326
PPP CHAP, 337-338
PPP PAP, 337-338
SNMPv3, 665, 672-673
authentication ppp pap command, 328
authenticators, switches as, 137
auto-cost reference-bandwidth command, 211, 609
autonomous system (AS), 164-165, 288
auto-summary command, 253, 259
EIGRP, 235
EIGRP for IPv4, 614
autosummarization, 252
classful network boundaries, 252-253
discontiguous classful networks, 253-254
AWS (Amazon Web Services), 705

B

backbone areas, 179
multiarea on ABR configuration, 591
super, 361
backbone routers, 179
backup DRs (BDRs), 174, 198-199
backup port role (RSTP), 55
backup ports, 53, 83
bandwidth
EIGRP
for IPv6 routes, 616-617
metrics, 224-227, 251
routes, tuning, 246
interfaces
defaults, 203
higher, 204
OSPF costs based on, 202-203
least-bandwidth, 224
managing, 465
MetroE, 355
reference, 203-204
bandwidth command, 203, 211, 258, 343
EIGRP, 235, 614
for IPv6, 630
metrics, 224, 251
OSPFv3 interface, 609
batch traffic, 467
BDRs (backup DRs), 174, 198-199
Bellman-Ford protocols. *See* DV protocols
best path selection (BGP), 289-290
BGP (Border Gateway Protocol), 165, 286
AS, 288
ASNs, 288
best path selection, 289-290
configuring, 293-294
external. *See* eBGP
IGPs, compared, 287
internal (iBGP), 288-289
ISP default routes, learning, 303-304

neighbors, 287
prefixes, 288
reachability, 287
route advertising, 287-288
routing table analysis reports website, 287
table entries, injecting, 298
advertising subnets to ISPs, 300-301
classful network routes, 298-300
static discard routes, 301-303
update messages, 287, 294
bgp commands, 295
BIDs (bridge IDs)
STP, 43
root switch election, 44-45
verification, 70
system ID extensions, 67
binary-to-hexadecimal conversion, 767
binary wildcard masks, 423
blocking state
interfaces, 41-43
RSTP ports, 84
Border Gateway Protocol. *See* BGP
BPDU (bridge protocol data unit), 43
BPDU Guard, 58
configuring, 74
enabling/disabling, 75
global settings, displaying, 76
verifying, 75
branch offices public cloud example, 711-713
bridge IDs. *See* BIDs
bridges. *See* switches
broadcast storms, 39-41
burned-in MAC addresses, 43

C

cable Internet, 371
cabling
DTE cables, 319
leased-line WANs, 316-317
stacking cables, 147
CAC (Call Admission Control) tools, 479
carrier Ethernet, 348
Catalyst switches RSTP modes, 80-82
Catalyst switches STP modes, 80-81
CBWFQ (Class-Based Weighted Fair Queuing), 478
***CCNA ICND2 200-105 Official Cert Guide Premium Edition eBook and Practice Test*, 755**
CCNA (ICND2) Config Labs website, 758
CCNA R&S practice exam, 753
CE (customer edge), 358
centralized control planes, 729
CFN (Cisco Feature Navigator), 503
challenge messages, 325
channel-group command (EtherChannels), 77, 89, 515
incorrect options, troubleshooting, 98-100
Layer 3, troubleshooting, 511
channel service unit (CSU)/data service unit (DSU), 316
CHAP (Challenge Handshake Authentication Protocol)
authentication, 325, 337-338
configuring, 327
verifying, 328
chassis aggregation, 149
benefits, 151
design, improving, 150
distribution/core switches high availability, 149-150
switch stacking, 149-151
CIR (committed information rate), 355, 481
Cisco
Access Control Server (ACS), 139
Application Centric Infrastructure (ACI), 734-735
BPDU Guard, 58
Catalyst switches RSTP modes, 80-82
Catalyst switches STP modes, 80-81

DevNet, 737
Feature Navigator (CFN), 503
Intercloud Fabric, 711
nondisclosure agreement (NDA), 752
Open SDN Controller (OSC), 734
Prime management products website, 661
server hardware, 697
Unified Communication Manager (CUCM), 29
virtual ASA firewall (ASAv), 715

Class-Based Weighted Fair Queuing (CBWFQ), 478

Class of Service (CoS) field (802.1Q header), 473

Class Selector (CS), 476

classful networks
autosummarization at boundaries, 252-253
discontiguous, 253-254
routes, injecting, 298-300

classful routing protocols, 167, 252

classic mode (EIGRP configuration), 237

classification (QoS), 469
ACLs, 471
matching, 470
with marking, 470
NBAR, 471-472
routers, 469-471

classless routing protocols, 167

clear ip ospf process command, 192, 212

clear-text passwords, 664

CLI skills, 757-758

client VPNs, 375-376

clock rate commands, 332, 343

clocking, 316

cloud computing
address assignment services, 717-718
cloud services catalogs, 703
Cloud Services Routers (CSRs), 709
DHCP services, 718
Infrastructure as a Service (IaaS), 705
NTP, 718-719
Platform as a Service (PaaS), 706-707
private, 703-704
public, 704
accessing with Internet, *707-709*
accessing with private VPNs, *709*
accessing with private WANs, *709-711*
branch offices example, *711-713*
DNS services, *716-717*
email services traffic flow, *712-713*
intercloud exchanges, *710-711*
Internet connections, *713*
private WAN connections, *713*
VNFs, *714-716*
services, 702-703
Software as a Service (SaaS), 706

Cloud Services Routers (CSRs), 709

codecs, 467

commands
aaa authentication login default, 141
aaa new-model, 140
access-class, 461
access-list, 421-423, 433-439, 461
any keyword, *423-424*
building ACLs with, *428-429*
deny keyword, *424*
examples and logic explanations, *440-441*
extended numbered ACL configuration commands, *441*
log keyword, *427*
permit keyword, *421*, *424*
reverse engineering from ACL to address range, *429-430*
tcp keyword, *438*
upd keyword, *438*
authentication ppp pap, 328
auto-cost reference-bandwidth, 211, 609
auto-summary, 253, 259
EIGRP, *235*
EIGRP for IPv4, *614*
bandwidth, 203, 211, 258, 343
EIGRP, *235*, *614*
EIGRP for IPv6, *630*

EIGRP metrics, *224*, *251*
OSPFv3 interface, *609*
bgp, 295
channel-group (EtherChannels), 77, 89, 515
incorrect options, *troubleshooting*, *98-100*
Layer 3, *troubleshooting*, *511*
clear ip ospf process, 192, 212
clock rate, 332, 343
command, 211
configure terminal, 23
debug, 273
debug eigrp fsm, 259
debug eigrp packets, 272, 285
debug ip ospf adj, 285
mismatched OSPF areas, *276*
OSPF neighbors, *troubleshooting*, *275*
debug ip ospf events, 285
debug ip ospf hello, 285
Hello/dead timer mismatches, *279*
OSPF neighbors, *troubleshooting*, *275*
debug ip ospf packet, 285
debug ipv6 ospf adj, 597
debug ppp authentication, 337, 344
debug ppp negotiation, 344
debug spanning-tree events, 72, 90
default-information originate, 201, 211, 304, 593
default-information originate always, 201
delay, 235, 258
EIGRP, *614*
EIGRP for IPv6, *630*
EIGRP metrics, *224*, *251*
deny, 445-447, 461
extended IPv6 ACLs, *640*
IPv6 ACLs, *638*
deny icmp any any, 647
description, 343
dialer pool, 393, 410
dns-server, 540
eigrp router-id, 235, 240
EIGRP, *614*
EIGRP for IPv6, *630*
encapsulation, 343, 497
encapsulation dot1q, 515
encapsulation ppp, 327, 332, 393, 410
erase startup-config, 126
frequency, 693
history buckets-kept 6, 693
history enhanced, 680
history enhanced interval, 693
history filter all, 693
history lives-kept 1, 693
hostname, 327
icmp-echo, 693
ifconfig, 537, 569, 583
interface, 20, 31, 515
interface dialer, 410
interface loopback, 185, 211
interface multilink, 343
interface multilink1, 332
interface port-channel, 515
interface range, 22
interface tunnel, 379, 410
interface vlan, 515
ip -6 neighbor show, 583
ip access-group, 426, 433, 441, 450, 461
ip access-list, 445, 461
ip access-list extended, 446
ip address, 538, 551-552
IP addresses on loopback interfaces, *185*
MLPPP, *332*
subinterfaces, *497*
ip address negotiated, 394, 410
ipconfig, 537, 569, 583
ip domain-lookup, 540-541
ip hello-interval eigrp, 235, 258, 284, 614
ip helper-address, 542-543
ip hold-time eigrp, 235, 258, 284
ip mtu, 281, 601
ip name-server, 540
ip ospf, 211

ip ospf cost, 211
ip ospf dead-interval, 284
ip ospf hello-interval, 284
ip route, 307
ip routing, 515
ip sla, 693
ip sla restart, 693
ip sla schedule, 678
ipv6 access-list, 644, 653
ipv6 access-list deny, 644
ipv6 access-list permit, 644
ipv6 address, 567, 583
ipv6 dhcp relay destination, 583
ipv6 eigrp, 614, 630
ipv6 hello-interval eigrp, 630
ipv6 hold-time eigrp, 630
ipv6 mtu, 601
ipv6 ospf, 589, 609
ipv6 ospf cost, 609
ipv6 router eigrp, 614, 630
ipv6 router ospf, 589, 609
ipv6 traffic-filter, 639, 653
ipv6 unicast routing, 567, 583
mac-address, 410
maximum-paths, 204
defined, *211*, *258*
EIGRP, *235*, *614*
EIGRP for IPv6, *618*, *630*
EIGRP load balancing, *249*
OSPFv3, *592*, *609*
monitor session, 684, 694
mtu, 410
name, 20, 36, 126
ndp -an, 583
neighbor, 307
neighbor shutdown, 297
netsh interface ipv6 show neighbors, 583
network
BGP, *307*
BGP table entries, *injecting*, *298-303*
EIGRP, *235-237*, *258*
EIGRP for IPv4, *614*
EIGRP for IPv6 compatibility, *614*
OSPF single-area configuration, *187-188*
OSPFv2 interface configuration, *205*
OSPFv2 multiarea configuration, *197*
no auto-summary, 254
no ip access-group, 449
no ip address, 510
no ip domain-lookup, 541
no ip sla schedule 1, 678
no neighbor shutdown, 297
no passive-interface, 211, 259
no shutdown, 36, 343
EIGRP for IPv6, *630*
EIGRP for IPv6 routing, *616*
Layer 1 leased-line WAN problems, *336*
OSPF processes, *280*
ROAS subinterfaces, *499*
no spanning-tree portfast bpduguard default, 89
no spanning-tree portfast default, 89
no switchport
Layer 3 EtherChannels, *510*
Layer 3 switches, *515*
routed ports, *506*
passive-interface, 193, 211, 284
EIGRP, *239*, *259*
OSPF interfaces as passive, *configuring*, *185*
OSPFv3, *589*
passive-interface default, 193, 259
permit, 445-447, 461
extended IPv6 ACLs, *640*
GRE tunnel ACLs, *387*
IPv6 ACLs, *638*
permit gre, 410
permit icmp any any router-advertisement, 648
permit icmp any any router-solicitation, 648
permit ipv6, 653

ping, 455, 540-543, 583
IPv6 host connectivity, testing, 570
IPv6 routes, testing, 571, 583
leased-line WANs, 335
self-ping, 456-457
ping6, 583
IPv6 ACLs, 639
IPv6 connectivity, testing, 570
ppp authentication, 332, 343
ppp authentication chap, 327
ppp chap hostname, 410
ppp chap password, 410
ppp multilink, 332, 344
ppp multilink group, 344
ppp multilink group 1, 332
ppp pap sent-username, 328, 343
pppoe-client dial-pool-number, 393, 410
pppoe enable, 394, 410
remark, 445, 461
router bgp, 294-295
router eigrp, 235, 258, 614
router-id, 211
OSPFv3, 589, 609
RIDs, defining, 185
router ospf, 185, 211
router ospf 1, 186
sdm prefer, 503
sdm prefer lanbase-routing, 515
show
IPv6 ACLs, 639
routing protocol-enabled interfaces, verifying, 262
STP status, 64
show access-list, 446
show access-lists, 425, 434, 452, 461, 653
show arp, 541
show controllers, 334
show controllers serial, 344
show etherchannel, 90, 515
show etherchannel summary, 100, 510
show etherchannel 1 summary, 78
show interfaces, 285, 344, 515, 538
EIGRP neighbor requirements, verifying, 272
MLPPP, 334
OSPF interfaces, troubleshooting, 270
OSPF neighbors, troubleshooting, 275
OSPFv3 interface bandwidth, 604
PPP CHAP status, 328
PPP PAP, 329
routed ports, 507
show interfaces description, 285, 545
show interfaces dialer, 397, 410
show interfaces PPP status, 327
show interfaces status
Layer 3 EtherChannels, 510
routed ports, 507
show interfaces switchport, 26-28, 31, 36, 106-108, 126
show interfaces trunk, 26-28, 32, 36, 108
show interfaces tunnel, 383, 410
show interfaces virtual-access, 410
show interfaces virtual-access configuration, 398
show interfaces vlan, 515
show ip access-list, 434, 447-449
show ip access-lists, 425, 452, 461
show ip bgp, 308
show ip bgp summary, 296, 308
show ip eigrp interfaces, 259, 284
EIGRP-enabled interfaces, 238-239, 262
EIGRP neighbor requirements, verifying, 272
multilink interfaces, 333
show ip eigrp interfaces detail, 238, 259
show ip eigrp neighbors, 259, 284
neighbor status, displaying, 240
neighbor verification checks, 272
show ip eigrp topology, 259
metrics, 248
successor routes, 245
topology table, 243
show ip eigrp topology all-links, 247

show ip eigrp topology command, 246
show ip interface, 426, 434, 451-452
show ip interface brief, 344
GRE tunnels, 382
multilink interfaces, 333
OSPF interfaces, troubleshooting, 270
show ip interfaces, 272
show ip ospf, 211, 285
duplicate OSPF RIDs, 277
OSPF neighbors, troubleshooting, 275
show ip ospf database, 169, 189, 212
show ip ospf interface, 211, 285
DRs/BDRs details, displaying, 198
Hello/dead timer mismatches, 279
OSPF areas for ABR interfaces, 198
OSPF neighbors, troubleshooting, 275
OSPFv2 interface configuration, 207
passive interface, 193
show ip ospf interface brief, 193, 211, 284
OSPF areas for ABR interfaces, 198
OSPF-enabled interfaces, identifying, 262
OSPF neighbors, troubleshooting, 275
OSPF status on interfaces, 268
OSPFv2 interface configuration, 207
show ip ospf neighbor, 172, 211, 285
DRs/BDRs details, displaying, 198
neighbors, listing, 274
OSPF processes shutdown, 280
show ip ospf neighbor interface brief, 280
show ip protocols, 211, 259, 284
EIGRP enabled interfaces, 239-240, 262
EIGRP neighbor requirements, verifying, 272
EIGRP neighbor status, displaying, 241
IPv4 routing protocols, 190
OSPF configuration errors, 269-270
OSPFv2 interface configuration, 206
show ip route, 212, 259, 308, 546-548
administrative distance, 168
dialer interface Layer 3 orientation, 400
EIGRP-learned routes, displaying, 242
IPv4 routes added by OSPF, 190
routing tables, displaying, 515
show ip route eigrp, 242, 259, 284
show ip route ospf, 212, 285, 546
show ip route static, 201
show ip sla enhanced-history distribution-statistics, 694
show ip sla history, 680, 694
show ip sla statistics, 694
show ip sla summary, 694
show ipv6 access-list, 653
show ipv6 access-lists, 643
show ipv6 eigrp interfaces, 620, 630
show ipv6 eigrp interfaces detail, 630
show ipv6 eigrp neighbors, 630
show ipv6 eigrp topology, 631
show ipv6 eigrp topology | section, 631
show ipv6 interface, 583, 653
show ipv6 neighbors, 583
IPv6 ACL ICMPv6 NDP message filtering, 646
IPv6 IPv4 replacement, 572
show ipv6 ospf, 604, 610
show ipv6 ospf database, 600, 610
show ipv6 ospf interface, 595-596, 610
show ipv6 ospf interface brief, 610
OSPFv3 interface costs, 604
OSPFv3 interfaces, 595
show ipv6 ospf neighbor, 599, 610
show ipv6 protocols, 583, 610
EIGRP for IPv6, 630
EIGRP for IPv6 interfaces, 620
OSPFv3 interfaces, 595
show ipv6 route, 583, 610
EIGRP for IPv6, 631
IPv6 router connectivity, 572
show ipv6 route eigrp, 631
show ipv6 route ospf, 603, 610
show ipv6 route | section, 631
show ipv6 routers, 583, 646
show mac address-table, 106
show mac address-table dynamic, 103
show monitor detail, 687, 694

show monitor session, 687, 694
show monitor session all, 686
show ppp all, 328-329, 344
show ppp multilink, 334, 344
show pppoe session, 399, 410
show running-config, 126, 424, 446-448
show snmp, 668, 694
show snmp community, 667, 694
show snmp contact, 694
show snmp group, 673, 694
show snmp host, 667, 694
show snmp location, 694
show snmp user, 673, 694
show spanning-tree, 90
show spanning-tree bridge, 74
show spanning-tree interface, 90
show spanning-tree interface detail, 75
show spanning-tree root, 70, 74
show spanning-tree summary, 76, 90
show spanning-tree vlan, 90
show spanning-tree vlan 10, 68-70
show spanning-tree vlan 10 bridge, 70
show spanning-tree vlan 10 interface gigabitethernet0/2 state, 84
show standby, 525, 529, 535
show standby brief, 524, 535
show tcp brief, 296
show tcp summary, 308
show vlan, 36, 106, 134
show vlan brief, 21-24, 106
show vlan id, 22, 106
show vlan status, 126
show vlans, 499, 515
show vtp password, 126, 134
show vtp status, 24, 36, 123, 126, 134
shutdown, 36, 343
EIGRP for IPv6, 630
EIGRP for IPv6 routing, 616
Layer 1 leased-line WAN problems, 336
OSPF processes, 280
ROAS subinterfaces, 499
shutdown vlan, 126, 134
snmp-server, 666
snmp-server community, 693
snmp-server contact, 693
snmp-server enable traps, 693
snmp-server group, 669-670
snmp-server host, 666, 674, 693
snmp-server location, 693
snmp-server user, 671-672
spanning-tree, 89
spanning-tree bpduguard disable, 89
spanning-tree bpduguard enable, 68, 74, 89
spanning-tree mode, 80, 89
spanning-tree mode mst, 66
spanning-tree mode pvst, 66
spanning-tree mode rapid-pvst, 66, 82
spanning-tree pathcost method long, 48
spanning-tree portfast, 68, 74, 89
spanning-tree portfast bpduguard, 89
spanning-tree portfast default, 75, 89
spanning-tree portfast disable, 75, 89
spanning-tree vlan, 67
spanning-tree vlan 10 port-priority 112, 96
speed, 545
standby, 523, 535
standby 1 preempt, 527
standby version, 528
standby version 1 | 2, 535
switchport, 506, 515
switchport access vlan, 20, 23, 31, 36, 105, 126
switchport mode, 25, 36
switchport mode access, 20, 23, 31, 130
switchport mode dynamic auto, 107
switchport mode dynamic desirable, 27
switchport mode trunk, 24, 108, 496
switchport nonegotiate, 28, 36, 108, 130
switchport trunk allowed vlan, 36, 109
switchport trunk encapsulation, 25, 36
switchport trunk native vlan, 36, 110
switchport voice vlan, 30-31, 36, 126

traceroute, 543
GRE tunnels, 384
IPv6 host connectivity, testing, 570
IPv6 network router problems, troubleshooting, 579
IPv6 router connectivity, testing, 571
IPv6 routes, testing, 583
traceroute6, 583
tracert, 583
tunnel destination, 384-386, 409
tunnel mode gre ip, 382, 410
tunnel mode gre multipoint, 382
tunnel source, 384, 409
undebug all, 285
username, 327, 343
variance, 258
EIGRP, 235, 250, 614
EIGRP for IPv6, 618, 630
verification, 68
vlan, 20, 31, 36, 126
vlan 10, 115
vlan 200, 128
vtp, 125
vtp domain, 126, 133
vtp mode, 36, 126, 133
vtp mode off, 24, 126
vtp mode transparent, 24, 126
vtp password, 126, 133
vtp pruning, 126, 134
vtp version, 133
committed information rate (CIR), 355, 481
communities (SNMP), 664
Community-based SNMP Version 2 (SNMPv2c), 664
community strings (SNMP), 664
confidentiality (Internet VPNs), 373
Config Checklist app, 758
configure terminal command, 23
configuring
AAA servers, 140-142
AAA servers for 802.1x, 137
ACLs (access control lists)
extended numbered, 441-444
named, 445-446
numbered, 448-449
standard numbered ACLs, 424-427
BGPs, 293
disabling eBGP neighbors, 297
eBGP neighbor verification, 296-297
eBGP neighbors using link addresses, 294-295
ISP default routes, learning, 303-304
table entries, injecting, 298-303
transporting messages with TCP, 294
update messages, 294
BPDU Guard, 74-75
DHCP snooping, 144-145
EIGRP, 235
ASNs, 235
checklist, 235
classful network numbers, 236
classic versus named mode, 237
sample internetwork, 235
verification. See *verifying, EIGRP configuration*
wildcard masks, 236-237
EIGRP for IPv6, 613
commands, 614
example, 614-616
load balancing, 617-618
route metrics, 616-617
timers, 618
EtherChannels, 76-79
GRE tunnels, 380-382
HDLC, 321-323
HSRP, 523-524, 529-530
ICMP-Echo operations, 678
IGPs, 293
interfaces as passive, 193
IPv6
addressing on routers, 568
extended ACLS, 640-642
hosts, 565-567
routing, 567

standard ACLs, *637-640*
static routes, *568-569*
ISL, 497
ISP routers, 395
Layer 3
EtherChannels, *508-509*
switch routed ports, *506-508*
switching with SVIs, *501-502*
local SPAN, 684-687
MLPPP, 332
multiarea OSPFv2, 194-197
network commands, *197*
single-area configurations, *195-196*
subnets, *194*
verifying, *197-200*
OSPFv2 interfaces, 205-207
OSPFv3, 587
default routes, *593*
load balancing, *592*
multiarea example, *588*
multiarea on ABR, *590-591*
route selection metrics, *setting*, *592*
single-area, *589-590*
overlapping VLSM subnets, 551-552
PortFast, 74-75
PPP, 326-330
CHAP, *327*
PAP, *328-330*
PPPoE, 392
ISP router configuration example, *395*
Layer 1, *393*
Layer 2, *393-394*
summary, *394-395*
verification, *396-401*
RIDs (OSPF), 191-192
ROAS, 496
native VLANs, *497-498*
subinterfaces, *496-497*
troubleshooting, *500*
verifying, *498-499*
single-area OSPFv2, 186-187
IPv4 addresses, *186*
matching with network command, *187-188*
multiarea configurations, *195-196*
network command, *187*
organization, *185*
passive interfaces, *192-193*
RIDs, *191-192*
verifying, *188-190*
wildcard masks, *187-188*
SNMPv2
Get/Set messages, *665-666*
Trap/Inform messages, *666-667*
verifying, *667-669*
SNMPv3, 669
authentication, *672-673*
encryption, *672-673*
groups, *669-671*
notifications, *674-675*
requirements, *669*
summary, *675-676*
users, *672*
verifying, *673*
STP, 65
modes, *65-66*
options, *68*
per-VLAN port costs, *68*
port costs, *71-72*
PVST+, *66-67*
root election influence, *72-74*
system ID extensions, *67*
topology changes, *influencing*, *48-49*
verification commands, *68*
VLANs (virtual LANs), 20
data and voice VLANs, *30-32*
full VLAN configuration example, *20-23*
shorter VLAN configuration example, *23-24*
trunking, *24-28*

VTP
common rejections, troubleshooting, 128
default VTP settings, 121
example, 122
new VTP configuration settings, 122
planning, 121
steps, 121
storing configuration, 125-126
transparent mode, 126
congestion
avoidance, 484-485
management, 477-479
connections (public cloud access)
branch offices, 713
Internet, 707-709
private WANs, 709-711
VPNs, 709
contiguous networks, 253
control planes
centralized, 729
distributed, 729
networking devices, 726-727
control protocols (CP), 324
controllers, 728
APIC-EM, 738
centralized control, 729
Northbound Interfaces (NBIs), 730-732
OpenDaylight SDN controller, 733
Southbound Interfaces (SBIs), 729-730
convergence
EIGRP, 227
DUAL process, 229-230
feasible successor routes, 247-248
successors, 228-229
routing protocols, 164
STP, 42, 98
converting
binary to hexadecimal, 767
decimal to binary, 764-766
hexadecimal to binary, 767
core switches, 149-150
CoS (Class of Service) fields (802.1Q header), 473-474
costs. *See* metrics
counters
historical success/failure (IP SLAs), 679
IP SLA, 679-680
CP (control protocols), 324
CPE (customer premises equipment), 316
CS (Class Selector), 476
CS DSCP values, marking, 476
CSRs (Cloud Services Routers), 709
CSU/DSU (channel service unit/data service unit), 316-318
CUCM (Cisco Unified Communication Manager), 29
customer edge (CE), 358

D

data
application traffic, 466-467
EIGRP for IPv6 topology, 623-624
integrity, 373
usage (MetroE), 354-356
data centers (virtual)
networking, 699
physical networks, 700
vendors, 699
workflow, 701-702
data circuit-terminating equipment (DCE), 318
data plane
EtherChannel impact on MAC tables, 103-104
networking devices, 725-726
STP impact on MAC tables, 102
VLAN of incoming frames, 104-105
data terminal equipment (DTE), 318
databases
LSDB
area design, 179
best routes, finding, 170
contents, displaying, 189
exchanging between neighbors, 173-175

LSAs relationship, *169*
OSPFv3, *600-601*
MIB, 661-663
OIDs, *663*
variable numbering/names, *663*
variables, *monitoring*, *662*
views, *670*
topology, 177
VLAN, 123-125
DCE (data circuit-terminating equipment), 318
Dead Interval timer, 174
dead timers, 279-280
debug command, 273
debug eigrp fsm command, 259
debug eigrp packets command, 272, 285
debug ip ospf adj command, 285
mismatched OSPF areas, 276
OSPF neighbors, troubleshooting, 275
debug ip ospf events command, 285
debug ip ospf hello command, 285
Hello/dead timer mismatches, 279
OSPF neighbors, troubleshooting, 275
debug ip ospf packet command, 285
debug ipv6 ospf adj command, 597
debug messages, 248
debug ppp authentication command, 337, 344
debug ppp negotiation command, 344
debug spanning-tree events command, 72, 90
decimal-to-binary conversion, 764, 766
decimal wildcard masks, 421-423
default-information originate always command, 201
default-information originate command, 211, 304
OSPF default routes, 201
OSPFv3, 593
default routes, 593
default VLANs, 20
delay command, 258
EIGRP, 235, 614
EIGRP for IPv6, 630
EIGRP metrics, 224, 251
delays
EIGRP
for IPv6 routes, *616-617*
metrics, *224*, *251*
managing, 465
delivery headers, 379
deny command, 445-447, 461
extended IPv6 ACLs, 640
IPv6 ACLs, 638
deny icmp any any command, 647
deny keyword, 418, 424
dependencies (SPAN), 684-685
description command, 343
design
improving with chassis aggregation, 150
Internet edge, 290
MetroE Layer 3, 352
E-LAN service, *353*
E-Line service, *352-353*
E-Tree service, *353-354*
MetroE physical, 347-348
MPLS Layer 3, 358
MPLS VPNs Layer 3, 360-363
OSPF area, 179
ABR, *179*
areas, *178-179*
backbone areas, *179*
backbone routers, *179*
benefits, *180*
interarea routes, *179*
internal routers, *179*
intra-area routes, *179*
MPLS VPNs, *361-362*
network size, *178*
problems, *177*, *268*
single-area, *177*
SPF workload, *reducing*, *179*
three-area, *178*
OSPFv3 multiarea, 588

designated ports. ***See*** **DPs**
designated routers. ***See*** **DRs**
destination addresses, 384
destination IP, matching, 437-438
destination ports (SPAN), 683
devices, networking, 725
control, centralizing, 729
control plane, 726-727
data plane, 725-726
management plane, 727
switch internal processing, 727-728
DevNet, 737
DHCP (Dynamic Host Control Protocol)
Binding Table, 145
DHCP Relay, 542
public cloud services, 718
snooping
configuration settings, 144
DHCP-based attacks, 143-144
DHCP Binding Table, 145
features, 142
ports as trusted, configuring, 144
rate limiting, 145
rules summary, 144
trusted/untrusted ports, 143-145
stateful, 576-577
troubleshooting, 542-543
DHCP-based attacks, 143-144
DHCPv6, 565-566
dialer interfaces
Layer 3 orientation, 400
PPPoE
configuration, 393
verifying, 397-398
dialer pool command, 393, 410
Differentiated Services Code Point. ***See*** **DSCP**
Diffusing Update Algorithm (DUAL), 229-230, 613
Digital Signal level 0 (DS0), 318
Digital Signal level 1 (DS1), 318
Digital Signal level 3 (DS1), 318
digital subscriber lines (DSLs), 370-371
Dijkstra SPF algorithm, 170
direction (ACLs), 417-418
disabling
BGP neighbors, 297
BPDU Guard, 75
DTP, 108
EIGRP for IPv6 routing, 616
PortFast, 75
ports, 53
VLANs, 106
VLAN trunking, 130
discard routes, 302
discarding state, 53
discontiguous networks, 252-254
discovery (EIGRP neighbors), 222
displaying
BPDU Guard global settings, 76
DRs/BDRs details, 198
EIGRP
enabled interfaces, 262
IPv4 routing table, 241-242
neighbor status, 240-241
topology table, 243-244
LSDB contents, 189
OSPF-enabled interfaces, 262
passive interfaces, 193
PortFast global settings, 76
TCP connections, 296
distance vector protocols. ***See*** **DV protocols**
distributed control planes, 729
distribution switches, chassis aggregation, 149-150
DMVPN (Dynamic Multipoint VPN), 389
DNS (Domain Name System)
IPv6 network troubleshooting, 575-576
public cloud, 716-717
troubleshooting, 540-541
dns-server command, 540
down status (interfaces), 336

DPs (designated ports), LAN segments, 42
choosing, 47, 96-98
problems, troubleshooting, 97
DRs (designated routers), 174
backup (BDRs), 174
discovering, 198-199
Ethernet links, 174-175
DROthers routers, 175
DS0 (Digital Signal level 0), 318
DS1 (Digital Signal level 1), 318
DS3 (Digital Signal level 3), 318
DSCP (Differentiated Services Code Point), 470
fields (QoS marking), 474
marking values, 475-476
DSLs (digital subscriber lines), 370-371
DSLAMs (DSL access multiplexers), 370
DTE (data terminal equipment), 318-319
DTP (Dynamic Trunking Protocol), 108
DUAL (Diffusing Update Algorithm), 229-230, 613
dual Internet edge design, 290
dual stack
OSPFv2/OSPFv3, 585
OSPFv3 address families, 586
strategies, 568
DV protocols, 216
distance/vector information learned, 216-217
EIGRP as, 220-221
route poisoning, 219-220
split horizon, 219
update messages, 217-219
dynamic EtherChannels configuration, 79
Dynamic Multipoint VPN (DMVPN), 389
Dynamic Trunking Protocol (DTP), 108

E

E1, 318
E3, 318
EAP (Extensible Authentication Protocol), 138
EAPoL (EAP over LAN), 138
earplugs (exam), 750
eBGP (External BGP), 288-289
Internet edge, 290
design, 290
enterprise public prefixes, advertising, 291-292
ISP default routes, learning, 292-293
neighbors
configuring, 295
disabling, 297
using link addresses, configuring, 294
verifying, 296-297
Eclipse IDE, 707
edge ports, 56
EF (Expedited Forwarding), 474
EF DSCP value marking, 475
EF RFC (RFC 3246), 475
EGP (exterior gateway protocol), 164, 287
EIGRP (Enhanced Interior Gateway Routing Protocol), 166
as advanced DV protocol, 220-221
authentication, 273
autosummarization, 252
classful network boundaries, 252-253
discontiguous classful networks, 253-254
benefits, 215-216
configuration, 235
ASNs, 235
checklist, 235
classful network numbers, 236
classic versus named mode, 237
sample internetwork, 235
wildcard masks, 236-237

convergence, 227
DUAL process, *229-230*
feasible successor routes, *247-248*
successors, *228-229*
disadvantages, 216
feasible successor routes
convergence, *247-248*
identifying, *245-247*
goals, 287
interfaces
configuration problems, *266-268*
identifying, *262*
OSPF interfaces, *compared*, *268*
troubleshooting, *263-268*
K-values, 273
metrics, 224
bandwidth, *251*
calculation, *224*
components, *248*
delay settings, *251*
EIGRP topology database, *248*
example, *225-226*
FD (feasible distance), *227-228*
RD (reported distance), *227-228*
route load balancing, *250*
serial link bandwidth, *226-227*
MPLS VPN challenges, 362-363
neighbors, 222-223
discovery, *222*
requirements, *271-272*
status, *221*, *240-241*
topology information, *exchanging*, *223-224*
troubleshooting example, *273-274*
verifying, *222*, *272-273*
OSPF, compared, 214
query/reply messages, 230
RIDs, configuring, 240
RIP metrics, compared, 166
RIPv2/OSPFv2, compared, 221
routes
choosing, *222*
load balancing, *249-251*
tuning with bandwidth changes, *246*
variance, *250-251*
successor routes, identifying, 244-245
topology
database metrics, *248*
exchange, *222*
table, *displaying*, *243-244*
variance, 250-251
verification, 237
EIGRP enabled interfaces, *finding*, *238-240*
IPv4 routing table, *displaying*, *241-242*
neighbor status, *displaying*, *240-241*
EIGRP for IPv6
configuration, 613
commands, *614*
example, *614-616*
load balancing, *617-618*
route metrics, *616-617*
timers, *618*
DUAL, 613
EIGRP for IPv4, compared, 612-613, 619
FS, 613
interfaces, 620-621
neighbors, 621-623
routes
ASNs, *615*
enabling/disabling, *616*
FS, *613*
successors, *613*
troubleshooting, *625-626*
verifying, *624-625*
topology data, 623-624
eigrp router-id command, 235, 240, 614, 630
E-LAN (Ethernet LAN) service, 350-353
E-Line (Ethernet Line) service, 349-353
email, 712-713
enabling
AAA servers, 140
BPDU Guard, 75

EIGRP, 235
EIGRP for IPv6 routing, 616
IPv6 routing, 567
OSPF configuration mode, 186
PortFast, 75
PPPoE, 394
VLANs, 106
Encapsulated RSPAN (ERSPAN), 684
encapsulation command, 343, 497
encapsulation dot1q command, 515
encapsulation ppp command, 327, 332, 393, 410
encryption
IPsec, 374-375
keys, 374
SNMPv3, 665, 672-673
tunnel VPNs, 374
***End-to-End QoS Network Design*, Second Edition (Cisco Press), 468**
end-user traffic, measuring, 677
endpoints, 735
enhanced history, 680
Enhanced Interior Gateway Routing Protocol. *See* EIGRP
***Enterprise QoS Solution Reference Network Design Guide*, 468**
enterprises, classification matching, 470
eq 21 parameters, 439
erase startup-config command, 126
ERSPAN (Encapsulated RSPAN), 684
EtherChannels, 57
configuring, 76-79
Layer 3
configuring, 508-509
troubleshooting, 511
verifying, 510
MAC tables impact, predicting, 103-104
troubleshooting, 98
configuration checks before adding interfaces, 100-101
incorrect options, 98-100
Ethernet
802.1Q headers, 473-474
802.11 headers, 474
access links, 348
carrier, 348
IEEE standards, 348
links, 174-175
WANs, 709
Ethernet LANs
service, 350-351
troubleshooting, 543-545
VLANs (virtual LANs)
configuration, 20-24
default VLANs, 20
IDs, 14
IP telephony, 28-32
native VLANs, 16
overview, 13-14
routing between, 16-19
tagging, 15
trunking, 14-28
Ethernet Line (E-Line) service, 349-350
E-Tree (Ethernet LAN) service, 351-354
ETSI (European Telco standards body), 716
EUI-64 rules, 567-568
EVC (Ethernet Virtual Connection), 350
exact IP address matching, 421
exam
CLI skills, 757-758
earplugs, 750
exam-day suggestions, 750-751
knowledge gaps, finding, 755-756
practice exams, 753-755
pre-exam suggestions, 750
preparing for failure, 751-752
question types, 748
ready to pass assessment, 759
scores, 759
study tasks, 760
studying after failing to pass, 759-760

time budget versus number of questions, 749
time-check method, 750
tutorial, 748-749
Expedited Forwarding (EF), 474
extended IPv6 ACLs
configuring, 640-642
examples, 642-643
extended numbered IPv4 ACLs, 437
configuration, 441-444
matching protocol, source IP, and destination IP, 437-438
matching TCP and UDP port numbers, 438-441
Extensible Authentication Protocol (EAP), 138
exterior gateway protocol (EGP), 164, 287
External BGP. *See* eBGP

F

Facebook (Wendell Odom), 761
failed interfaces, 43
failing the exam, 751-752, 759-760
failures
CHAP authentication, 337-338
HSRP, 521-522
keepalive, 336-337
PAP authentication, 337-338
FCS (Frame Check Sequence), 319
FD (feasible distance), 227-228, 244
feasibility conditions, 229, 247
feasible successor routes, 228-229
convergence, 247-248
identifying, 245-247
FHRP (First Hop Redundancy Protocol), 516
features, 520
HSRP, 521
active/passive model, 521
active/standby routers, choosing, 524
active/standby rules, 526
configuring, 523-524
failover, 521-522
group numbers, 524
load balancing, 522-523
with/without preemption, 526-527
troubleshooting, 528-531
verifying, 525
versions, 528
need for, 519
options, 520
fiber Internet, 372
FIFO (first-in, first-out), 477
filtering
ICMPv6 messages, 635, 645-648
IPv6
ACL policies, 634
issues, 573
finding
EIGRP
enabled interfaces, 238-240
feasible successor routes, 245-247
successor routes, 244-245
mismatched Hello/dead timers, 279
OSPF area mismatches, 276-277
routers best routes, 170
wildcard masks, 423
firewalls, 715
First Hop Redundancy Protocol. *See* FHRP
first-in, first-out (FIFO), 477
FlexStack, 149
FlexStack-Plus, 149
flooding, 169
flow
networking, 467
public cloud traffic, 712-713
Forward delay timer (STP), 49
forwarding
data. *See* routing
interface state, 41-43
paths, 738
forwarding plane. *See* data plane
Fractional T1, 318
Fractional T3, 318

Frame Check Sequence (FCS), 319
Frame Relay, 346
frames
broadcast storms, 39-41
defined, 469
HDLC, 320
incoming, 104-105
looping, 39
multiple frame transmissions, 41
PPP, 324
switching, 105
frequency command, 693
FS (feasible successor), 613
full drops, 485
full mesh topology (MetroE), 350
full neighbor state, 175, 594
full updates, 218, 223
full VLAN configuration example, 20-23
fully adjacent neighbors, 175, 598

G

generic routing encapsulation (GRE), 376
"Get IEEE 802" program, 52
Get messages
agent information, 662
RO/RW communities, 664
SNMPv2 support, 665-666
GLBP (Gateway Load Balancing Protocol), 516
global unicast addresses, 563
Google App Engine PaaS, 707
GRE (generic routing encapsulation), 376
GRE tunnels, 376
between routers, 377-378
configuring, 380-382
details, displaying, 382
functionality, testing, 384
large scale environments, 388
multipoint with DMVPN, 389
point-to-point, 378
routes, 383
troubleshooting, 384
ACLs, 387-388
interface state, 384-385
Layer 3 issues, 386
source/destination addresses, 384
tunnel destination, 385-386
tunnel interfaces, 377
unsecured networks, 378-380
verifying, 382-384
group numbers (HSRP), 524
groups
endpoint, 735
SNMPv3, 669-671

H

HDLC (High-level Data Link Control), 315, 319-323, 377
headers
802.1Q, 473-474
802.11, 474
delivery, 379
IP, 472-474
MPLS Label, 474
Hello BPDU, 43
Hello Interval, 221
Hello Interval timer, 174
Hello messages (OSPF), 171-172
Hello timer
dead timer mismatches, troubleshooting, 279-280
STP, 49
hexadecimal-to-binary conversion, 767
high availability, 149-150
High-level Data Link Control (HDLC), 315, 319-323, 377
High-speed WICs (HWICs), 317
historical success/failure counters (IP SLAs), 679
history
IP SLA data, 680-681
OSPF, 585
SNMP, 661

history buckets-kept 6 command, 693
history enhanced command, 680
history enhanced interval command, 693
history filter all command, 693
history lives-kept 1 command, 693
Hold Interval, 221
hostname command, 327
hosts
IPv6, 565
connectivity, verifying, 569-570
issues, 573
missing settings, 576-578
name resolution problems, 575-576
pings fail from default router, 574-575
pings only working in some cases, 573-574
stateful DHCPv6, 565-566
stateless address autoconfiguration (SLAAC), 566-567
routes, 339
server virtualization, 699
troubleshooting IPv4 settings
default router IP address setting, 541
DNS problems, 540-541
ensuring IPv4 settings match, 537-538
mismatched masks, 538-539
Hot Standby Router Protocol (HSRP), 516, 521
active/passive model, 521
active/standby routers, choosing, 524
active/standby rules, 526
configuration, troubleshooting, 529-530
configuring, 523-524
failover, 521-522
group numbers, 524
load balancing, 522-523
with/without preemption, 526-527
troubleshooting, 528
ACL blocks HSRP packets, 531
configuration, 529-530
group number mismatches, 531
misconfiguration symptoms, 530
routers configuring different VIPs, 531
version mismatches, 530-531
verifying, 525
versions, 528
HSRPv2 (HSRP version 2), 528
hub and spoke topology (MetroE), 351
Huston, Geoff website, 287
HWICs (High-speed WICs), 317
hypervisors, 699

I

IaaS (Infrastructure as a Service), 705
IANA (Internet Assigned Numbers Authority), 165
ASNs, assigning, 165
ICMPv6 parameters, 635
IPv6 multicast address space registry website, 647
website, 165
iBGP (Internal BGP), 288-289
icmp-echo command, 693
ICMP-Echo operations, 678
ICMP Echo probe, 677
icmp keyword, 454
ICMPv6
Echo Request messages, 640
messages, filtering, 635, 645-649
packets, matching, 641
ICND2 practice exam. *See* practice exams
IEEE (Institute of Electrical and Electronics Engineers)
802.1D Spanning-Tree states, 51
802.1D standard, 51
802.1w amendment, 51
802.1x
access, securing, 137
authenticators, 137
LAN access, securing, 137-138
default port costs, 48
Ethernet standards, 348
"Get IEEE 802" program, 52

ifconfig command, 537, 569, 583
IGP (interior gateway protocol), 164, 215
BGPs, compared, 287
classless/classful, 167
configuring, 293
goals, 287
metrics, 166-167
routing protocol algorithm, 165-166
subnets, 288
IGRP (Interior Gateway Routing Protocol), 166
implicit filtering, 648-649
incoming frames, 104-105
inferior Hello, 44
infinity, 219
Inform messages, 662-663
SNMPv2, 666-667
SNMPv3, 674-675
Infrastructure as a Service (IaaS), 705
injecting BGP table entries, 298
advertising subnets to ISPs, 300-301
classful network routes, 298-300
static discard routes, 301-303
instantiating VMs, 705
Integrated Intermediate System to Intermediate System (IS-IS), 166
interactive data application traffic, 466
interactive voice traffic, 468
interarea routes, 179, 199-200, 604
intercloud exchanges, 710-711
Intercloud Fabric, 711
interface command, 20, 31, 515
interface dialer command, 410
interface loopback command, 185, 211
interface multilink command, 343
interface multilink 1 command, 332
interface port-channel command, 515
interface range command, 22
interface tunnel command, 379, 410
interface vlan command, 515
interfaces
ABR OSPF areas, verifying, 198
access, 105-106
administratively shutdown, 43
application programming (APIs), 730
bandwidth
defaults, *203*
EIGRP metric calculations, *251*
EIGRP routes, *tuning*, *246*
higher reference, *204*
OSPF costs based on, *202-203*
blocking state, 41
delays, 251
dialer
Layer 3 orientation, *400*
PPPoE, *393*, *397-398*
down status, 336
EIGRP
configuration problems, *266-268*
enabled, *238-240*, *262*
OSPF interfaces, *compared*, *268*
troubleshooting, *263-268*
EIGRP for IPv6, 620-621
EtherChannels, adding, 100-101
failed, 43
forwarding state, 41
LAN speeds, 465
learning state, 51
listening state, 51
loopback, 191
multilink, 331
Northbound (NBIs), 730-732
OSPF
costs, *202-204*
EIGRP interfaces, *compared*, *268*
identifying, *262*
passive, *185*
troubleshooting, *268-270*
OSPFv2 configuration, 205-207
OSPFv3, 595
costs, *592*, *602-604*
troubleshooting, *596-597*
verifying, *595-596*

passive
EIGRP, *239*
OSPF, *192-193*
OSFPv3, *589*
per-VLAN STP costs, 68
routed, 506-508
routing protocol-enabled, verifying, 262
Southbound (SBIs), 729-730
states
changing with STP, *51*
forwarding or blocking criteria, *42-43*
status codes, 335
subinterfaces, 496-498
switched virtual. *See* SVIs
tunnel
ACLs, *387-388*
creating, *379*
destinations, *385-386*
Layer 3 issues, *386*
replacing serial links, *377*
state, *384-385*
virtual-access, 398
VLAN. *See* SVIs
WANs, 465
working, 43
interior gateway protocol. *See* IGP
Interior Gateway Routing Protocol (IGRP), 166
interior IP routing protocols, 221
Internal BGP (iBGP), 288-289
internal processing (switches), 727-728
internal routers, 179, 589-590
Internet
access, 369
cable Internet, *371*
DSLs (digital subscriber lines), *370-371*
fiber, *372*
WANs, *369*
wireless WANs, *371-372*
public cloud
accessing, *707-709*
computing branch office connections, *713*
VPNs, 369
benefits, *374*
clients, *375-376*
security, *373*
site-to-site, *374-375*
as WAN service, 369
wireless, 372
Internet Assigned Numbers Authority. *See* IANA
Internet edge, 290-293
Internet service providers. *See* ISPs
Inter-Switch Link (ISL), 16, 497
intra-area routes, 179
ip -6 neighbor show command, 583
ip access-group command, 426, 433, 441, 450, 461
ip access-list command, 445, 461
ip access-list extended command, 446
IP ACLs (access control lists). *See* ACLs
ip address command, 538, 551-552
IP addresses on loopback interfaces, 185
MLPPP, 332
subinterfaces, 497
ip address negotiated command, 394, 410
ip_address parameter, 187
IP addressing
conversions
binary-to-hexadecimal, *767*
decimal-to-binary, *764-766*
hexadecimal-to-binary, *767*
public clouds, 717-718
ip domain-lookup command, 540-541
IP headers, 472-474
ip hello-interval eigrp command, 235, 258, 284, 614
ip helper-address command, 542-543
ip hold-time eigrp command, 235, 258, 284
IP IGP metrics, 166-167
ip mtu command, 281, 601
ip name-server command, 540
ip ospf command, 211

ip ospf cost command, 211
ip ospf dead-interval command, 284
ip ospf hello-interval command, 284
ip route commands, 307
ip routing command, 515
IP SLAs (IP Service Level Agreements), 676
historical success/failure counters, 679
history data, troubleshooting with, 680-681
ICMP-Echo, 677-678
operations, 677
responders, 677
sources, 677
troubleshooting with
counters, 679-680
history data, 680-681
UDP Jitter probes, 677
ip sla command, 693
ip sla restart command, 693
ip sla schedule command, 678
IP telephony (VLANs), 28
data and voice VLAN concepts, 29-30
data and voice VLAN configuration and verification, 30-32
summary, 32
ipconfig command, 537, 569, 583
IPP (IP Precedence) fields (QoS marking), 474-476
IPsec, 374-375
IPv4 routing
ACLs, 633
address families, 585
EIGRP
configuration, 236-237
routing table, 241-242, 249-251
verification, 237-242
Layer 3 EtherChannels
configuring, 508-509
troubleshooting, 511
verifying, 510
Layer 3 switch routed ports, 505-508
Layer 3 switching with SVIs
configuring, 501-502
troubleshooting, 503-505
verifying, 502-503
matching addresses
any/all addresses, 423-424
exact IP address, 421
subset of address, 421-423
OSPF added, 190
OSPFv2 single-area configuration, 186
QoS marking, 472
routing protocols
displaying, 190
troubleshooting, 261-262
subnet masks
mismatched masks, 538-539
VLSM (variable length subnet masking), 549
troubleshooting
default router IP address setting, 541
DHCP issues, 542-543
DNS problems, 540-541
incorrect addressing plans, 549-552
IP forwarding issues, 545-548
LAN issues, 543-545
mismatched IPv4 settings, 537-538
mismatched masks, 538-539
packet filtering with access lists, 553
router WAN interface status, 552
ipv6 access-list commands
building, 644
IPv6 ACLs, 653
ipv6 access-list deny command, 644
ipv6 access-list permit command, 644
ipv6 address command, 567, 583
ipv6 dhcp relay destination command, 583
ipv6 eigrp command, 614, 630
ipv6 hello-interval eigrp command, 630
ipv6 hold-time eigrp command, 630
ipv6 mtu command, 601
ipv6 ospf command, 589, 609
ipv6 ospf cost command, 609

ipv6 router eigrp command, 614, 630
ipv6 router ospf command, 589, 609
IPv6 routing
access restrictions with IPv6 ACLs, 650
ACLs, 632-633
access-list commands, building, 644
access restrictions, 650
blocking, 647
capabilities, 635-636
extended, 640-643
filtering ICMPv6 NDP messages, 645-648
filtering policies, 634
ICMPv6 message filtering, 635
implicit filtering ICMPv6 NDP messages, 648-649
IPv4 ACL, compared, 633
limitations, 636-637
logging, 636
management control, 649-650
prefix lengths, 636
router originated packets, 637
standard, configuring, 637-640
testing, 643
tunneled traffic matching, 636
addressing on routers configuration, 568
connectivity, verifying, 569
hosts, 569-570
routers, 571-572
EIGRP
ASNs, 615
configuration, 613-616
DUAL, 613
EIGRP for IPv4, compared, 612-613, 619
FS, 613
interfaces, 620-621
load balancing, 617-618
neighbors, 621-623
routes, 616-617, 624-626
successors, 613
timers, 618
topology data, 623-624
global unicast addresses, 563
host configuration, 565
stateful DHCPv6, 565-566
stateless address autoconfiguration (SLAAC), 566-567
link-local addresses, 564
multicast addresses, 647
OSPF, 585-586
OSPFv3
configuration, 587-588
default routes, 593
interface cost metrics, 602-604
interfaces, 595-597
IPv6 MTU mismatches, 601-602
IPv6 routes, troubleshooting, 604-605
load balancing, 592
LSAs, 600
LSDBs, 600-601
multiarea on ABR configuration, 590-591
neighbors, 597-600
OSPFv2, compared, 587, 594
passive interfaces, 589
RIDs, 589
route selection metrics, 592
single-area configuration, 589-590
protocols, 585
QoS marking, 473
routers, enabling, 567
routes
EIGRP for IPv6 metrics, 616-617
OSPFv3 metrics, 592
static configuration, 568-569
subnetting, 563-564
troubleshooting, 572, 604-605
ACLs, 580
filtering issues, 573
host issues, 573
host pings fail from default router, 574-575
host pings only working in some cases, 573-574
missing IPv6 settings in host, 576-578

name resolution problems, 575-576
router issues, 573
routing, 579-580
unicast addresses, 563-565
ipv6 traffic-filter command, 639, 653
ipv6 unicast routing command, 567, 583
IS-IS (Integrated Intermediate System to Intermediate System), 166
ISL (Inter-Switch Link), 16, 497
ISPs (Internet service providers), 369
default routes, learning, 303-304
dial connections with PPP, 391
Internet edge, learning, 292-293
router configuration example, 395
subnets, advertising, 300-301

J

Jenkins continuous integration and automation tool, 707
jitter, managing, 465

K

keepalive failures, 336-337
keyboard, video display, or mouse (KVM), 697
keys (encryption), 374
keywords. *See also* commands
any, 423
deny, 418, 424
icmp, 454
log, 427, 636
permit, 418, 424
tcp, 438
udp, 438
knowledge gaps, finding, 755-756
K-values (EIGRP), 273
KVM (keyboard, video display, or mouse), 697

L

labs, completing, 757-758
LACP (Link Aggregation Control Protocol), 79
LANs, 495
defined, 13
DPs, 47, 96-98
interfaces, 465
redundancy, 38-41
security
IEEE 802.1x, 137-138
STP exposures, 58
troubleshooting, 543-545
VLAN support, adding, 115
Layer 1
leased-line WANs
CSU/DSUs, 318
physical components, 316-317
speeds, 317-318
troubleshooting, 335
leased-line WANs with HDLC, 319
PPPoE
configuration, 393
troubleshooting, 402-403
Layer 2
leased-line WANs, 336-338
leased-lines with HDLC, 319-320
MLPPP, 331
PPPoE
configuration, 393
troubleshooting, 403-404
switches, 17
Layer 3
GRE tunnel issues, 386
leased-line WANs, 338-339
MetroE design, 352
E-LAN service, 353
E-Line service, 352-353
E-Tree service, 353-354
MLPPP, 331
MPLS, 358

MPLS VPNs, 360-361
EIGRP challenges, *362-363*
OSPF area design, *361-362*
PPPoE
configuration, *394*
status, *verifying*, *400-401*
troubleshooting, *404*
switches, 17
EtherChannels, *508-511*
routed ports, *505-508*
with SVIs, *501-505*
VLAN (virtual LAN) routing, *19*
LCP (Link Control Protocol), 324-325
learning state, 51
leased-line WANs, 315
building, 319
CSU/DSU, 318
with HDLC, 319
configuring HDLC, *321-323*
de-encapsulating/re-encapsulating IP packets, *320*
framing, *320*
physical components, 316-317
with PPP
authentication, *325-326*
configuring PPP, *326-327*
configuring PPP CHAP, *327-328*
configuring PPP PAP, *328-330*
control protocols, *324*
framing, *324*
multilink. See *MLPPP*
PPP functions, *323*
speeds, 317-318
troubleshooting, 335
Layer 1 problems, *335*
Layer 2 problems, *336-338*
Layer 3 problems, *338-339*
mismatched subnets, *339*
least-bandwidth, 224
limiting SPAN sources, 687-688
Link Aggregation Control Protocol (LACP), 79
Link Control Protocol (LCP), 324-325
link-local addresses, 564
link-state advertisements. *See* LSAs
link-state database. *See* LSDB
link-state protocols, 166. *See also* OSPF
Link-State Update (LSU) packets, 173
links
access
MetroE, *348*
MPLS, *358*
addresses, 294-295
Ethernet, 174-175
RSTP types, 56
serial
bandwidth, *226-227*
replacing with IP tunnels, *377*
routing IP packets over, *376*
list logic (IP ACLs), 419-421
listening state (interfaces), 51
LLQ (Low Latency Queuing), 478-479
load balancing
EIGRP, 249-251
EIGRP for IPv6, 617-618
HSRP, 522-523
MLPPP, 331
OSPF, 204
OSPFv3, 592
local SPAN, configuring, 684-687
location (ACLs), 417-418
log keyword, 427, 636
log messages, unsolicited, 270
logging IPv6 ACLs, 636
logical switches, 148
logins (AAA), 139-142
Long-Term Evolution (LTE), 372
loopback interfaces, 191
looping frames, preventing, 39
loss, managing, 466
Low Latency Queuing (LLQ), 478-479
LSAs (link-state advertisements), 173
exchanging with OSPF neighbors, 173
DRs on Ethernet links, *174-175*
maintenance, *174*

flooding, 169
LSDB relationship, 169
OSPFv3, 600
router, 600
LSDB (link-state database), 169
area design, 179
best routes, finding, 170
contents, displaying, 189
exchanging between neighbors, 173-175
LSAs relationship, 169
OSPFv3, 600-601
LSU (Link-State Update) packets, 173
LTE (Long-Term Evolution), 372

M

mac-address command, 410
MAC addresses
burned-in, 43
forwarding, 103
learning, 103
tables
EtherChannel impact, predicting, 103-104
instability, 41
STP impact, predicting, 102
maintenance
EIGRP neighbors, 221
OSPF neighbors, 174
Managed Extensibility Framework (MEF), 349
Management Information Base. *See* MIB
management plane (networking devices), 727
managing
bandwidth, 465
delay, 465
IPv6 ACLs, 649-650
jitter, 465
loss, 466
SNMP, 661
manual EtherChannels configuration, 77-78
marking, 470-472
with classification, 470
DiffServ DSCP values, 475-476
Ethernet 802.1Q headers, 473-474
Ethernet 802.11 headers, 474
IP headers, 472-474
MPLS Label headers, 474
trust boundaries, 474
matching packets, 418
matching parameters
extended numbered ACLs
protocol, source IP, and destination IP, 437-438
TCP and UDP port numbers, 438-441
standard numbered ACLs
any/all addresses, 423-424
command syntax, 421
exact IP address, 421
subset of address, 421-423
wildcard masks, 421-423
MaxAge timer (STP), 49
maximum-paths command, 204, 211, 258
EIGRP
for IPv4, 235, 614
for IPv6, 618, 630
load balancing, 249
OSPFv3, 592, 609
maximum transmission unit (MTU), 224
measuring
cloud computing services, 703
end-user traffic, 677
MEC (Multichassis EtherChannel), 151
MEF (Managed Extensibility Framework), 349
memory (TCAM), 728
messages
challenge, 325
debug, 248
EIGRP, 230
Get
agent information, 662
RO/RW communities, 664
SNMPv2 support, 665-666

ICMPv6
Echo request, *640*
filtering, *635*
NDP, *filtering*, *645-649*
Inform, 662-663
SNMPv2 support, *666-667*
SNMPv3, *674-675*
NA (neighbor advertisement), 648
NS (neighbor solicitation), 648
OSPF Hello, 171-172
partial update, 220
RA (router advertisement), 648
RS (router solicitation), 648
RSTP, 55
Set
RO/RW communities, *664*
SNMPv2 support, *665-666*
writing variables on agents, *662*
SNMP variables, monitoring, 662
STP Hello BPDU, 43
Trap, 662-663
SNMPv2 support, *666-667*
SNMPv3, *674-675*
unsolicited log, 270
update
BGP, *287*, *294*
DV routing protocols, *217-219*
EIGRP, *223-224*

metrics
BGP best path selection, 289-290
EIGRP, 224
bandwidth, *251*
calculation, *224*
components, *248*
delay settings, *251*
EIGRP topology database, *248*
example, *225-226*
FD (feasible distance), *227-228*
RD (reported distance), *227-228*
route load balancing, *250*
serial link bandwidth, *226-227*
IGP, 166-167
infinity, 219
IPv6 routes
EIGRP for IPv6, *616-617*
OSPFv3 interface costs, *592*
OSPF, 202
based on interface bandwidth, *202-203*
higher reference bandwidth, *204*
setting, *204*
OSPFv3, 602-604
per-VLAN STP, 65-67

MetroE (Metro Ethernet), 346-347
access links, 348
data usage, 354-356
IEEE Ethernet standards, 348
Layer 3 design, 352-354
MEF, 349
physical design, 347-348
services, 349
E-LAN, *350-353*
E-Line, *349-353*
E-Tree, *351-354*
topologies
full mesh, *350*
hub and spoke, *351*
partial mesh, *351*
Point-to-Point, *349-350*

MIB (Management Information Base), 661-663
OIDs, 663
variables
monitoring, *662*
numbering/names, *663*
views, 670

mind maps, reviewing, 757

mismatched IPv4 settings, troubleshooting, 537-538

mismatched masks, troubleshooting, 538-539

mismatched subnets, 273

MLPPP (multilink PPP), 331
configuring, 332
Layer 2 fragmentation balance, 331
Layer 3, 331

load balancing, 331
verifying, 333-335
monitor session command, 684, 694
monitoring MIB variables, 662
MPBGP (Multiprotocol BGP), 360
MPLS (Multiprotocol Label Switching), 346, 356-357
access links, 358
Label headers, 474
Layer 3 design, 358
public cloud connections, 709
QoS, 359-360
Virtual Private Networks. *See* MPLS VPNs
MPLS VPNs (MPLS Virtual Private Networks), 357
EIGRP challenges, 362-363
Layer 3, 360-363
OSPF area design, 361-362
MST (Multiple Spanning Tree), 66
MTU (maximum transmission unit), 224
IPv6 mismatches, 601-602
OSPF mismatched settings, 281
mtu command, 410
multiarea on ABR OSPFv3 configuration, 590-591
multiarea OSPFv2 configuration, 194-197
network commands, 197
single-area configurations, 195-196
subnets, 194
verifying, 197-200
multiarea OSPFv3 configuration, 588
multicast addresses, 647
Multichassis EtherChannel (MEC), 151
multihomed Internet edge design, 290
multilayer switches. *See* Layer 3, switches
multilink interfaces, 331
multiple frame transmissions, 41
multiple queues (queuing systems), 477
multiple serial links between routers, 330
Multiple Spanning Tree (MST), 66
Multiprotocol BGP (MPBGP), 360
Multiprotocol Label Switching. *See* MPLS
multithreading, 698

N

NA (neighbor advertisement) messages, 648
name command, 20, 36, 126
named ACLs
configuration, 445-446
editing, 446-448
overview, 444-445
named mode (EIGRP configuration), 237
names (MIB variables), 663
National Institute of Standards and Technology (NIST), 702
native VLANs, 16
mismatched on trunks, 110
router configuration, 497-498
NBAR (Network Based Application Recognition), 471-472
NBIs (Northbound Interfaces), 730-732
NCP (Network Control Protocols), 324
NDA (nondisclosure agreement), 752
NDP (Neighbor Discovery Protocol), 563
filtering messages through IPv6 ACLs, 645-648
implicit filtering messages through IPv6 ACLs, 648-649
SLAAC, 566
ndp -an command, 583
neighbor commands, 307
neighbor shutdown command, 297
neighbors
BGP, 287, 297
eBGP
configuring, 295
disabling, 297
using link addresses, configuring, 294
verifying, 296-297

EIGRP for IPv4, 222-223
discovery, *222*
requirements, *272*
status, *221*, *240-241*
topology information, *exchanging*, *223-224*
troubleshooting, *273-274*, *277*
verifying, *222*, *272-273*
EIGRP for IPv6, 621-623
OSPF, 170-171
area mismatches, *finding*, *276-277*
duplicate RIDs, *277-279*
Hello messages, *171-172*
Hello/dead timer mismatches, *279-280*
LSDB exchange, *173-175*
meeting, *171*
requirements, *275*
RIDs, *learning*, *171*
states, *172*, *175*, *275*
troubleshooting, *274-280*
OSPFv3, 597
requirements, *598*
troubleshooting, *598-600*
verifying, *597-598*
relationships, 270-271
routing protocol relationships, troubleshooting, 262
states, 594

netsh interface ipv6 show neighbors command, 583

Network Based Application Recognition (NBAR), 471

network command, 211
BGP table entries, injecting, 298, 307
advertising subnets to ISPs, *300-301*
classful network routes, *298-300*
static discard routes, *301-303*
EIGRP, 235-237, 258, 614
OSPF single-area configuration, 187-188
OSPFv2
interface configuration, *205*
multiarea configuration, *197*

Network Control Protocols (NCP), 324

network functions virtualization (NFV), 716

network interface cards (NICs), 681, 699

Network Interface Modules (NIMs), 317

Network Layer Reachability Information (NLRI), 288

Network Management Station. ***See*** **NMS**

Network Time Protocol (NTP), 718-719

networks
analyzers, 682-683
broad access, 702
classful
autosummarization at boundaries, *252-253*
routes, *injecting*, *298-300*
contiguous, 253
controllers
centralized control, *729*
defined, *728*
Northbound Interfaces (NBIs), *730-732*
Southbound Interfaces (SBIs), *729-730*
devices, 725
control, *centralizing729*
control plane, *726-727*
data plane, *725-726*
management plane, *727*
security, *139-142*
switch internal processing, *727-728*
discontiguous, 252-254
flow, 467
physical data center, 700
programmability, 724
APIC Enterprise Module (APIC-EM), *735-737*
Application Centric Infrastructure (ACI), *734-735*
comparisons, *737*
public cloud
address assignment services, *717-718*
DHCP services, *718*
DNS services, *716-717*

NTP, *718-719*
VNFs, *714-716*
redundancy needs, 517-518
traffic
bandwidth, *managing*, *465*
characteristics, *465*
delay, *465*
jitter, *465*
loss, *466*
types, *466-468*
unsecured, 378-380
virtual, 699-700, 716
VMs, 700
Nexus 1000v vSwitch, 700
NFV (network functions virtualization), 716
NHRP (Next Hop Resolution Protocol), 389
NICs (network interface cards), 681, 699
NIMs (Network Interface Modules), 317
NIST (National Institute of Standards and Technology), 702
NLRI (Network Layer Reachability Information), 288
NMS (Network Management Station), 661
notification community strings, 667
SNMP, 661-663
no auto-summary command, 254
no ip access-group command, 449
no ip address command, 510
no ip domain-lookup command, 541
no ip sla schedule 1 command, 678
no neighbor shutdown command, 297
no passive-interface command, 211, 259
no shutdown command, 36, 343
EIGRP for IPv6, 616, 630
Layer 1 leased-line WAN problems, 336
OSPF processes, 280
ROAS subinterfaces, 499
no spanning-tree portfast bpduguard default command, 89
no spanning-tree portfast default command, 89
no switchport command
Layer 3 EtherChannels, 510
Layer 3 switches, 515
routed ports, 506
nondisclosure agreement (NDA), 752
noninteractive data application traffic, 467
nonroot switches (RPs), 94-96
problems, troubleshooting, 96
tiebreakers, 95-96
normal-time questions, 749
Northbound Interfaces (NBIs), 730
notification community strings, 667
notifications
SNMP, 662-663
SNMPv3, 674-675
NS (neighbor solicitation) messages, 648
NTP (Network Time Protocol), 718-719
numbered ACLs, configuration, 448-449
numbers
ASNs. *See* ASNs
HSRP group, 524
MIB variables, 663
ROAS subinterfaces, 497
sequence numbers, 446-448
numeric reference table
binary-to-hexadecimal conversion, 767
decimal-to-binary conversion, 764-766
hexadecimal-to-binary conversion, 767

O

ODL (OpenDaylight), 733-734
Odom, Wendell Twitter/Facebook information, 761
OIDs (object IDs), 663
on-demand self-service (cloud computing), 702
one-way delay, 465
ONF (Open Networking Foundation), 732

Open SDN, 732-733
Open SDN Controller (OSC), 734
Open Shortest Path First. *See* OSPF
OpenDaylight (ODL), 733-734
OpenFlow, 730-732
operations (IP SLAs), 677-678
OpFlex, 730
OSC (Open SDN Controller), 734
OSPF (Open Shortest Path First), 162, 169
area design, 179
ABR, 179, 198
areas, 178-179
backbone areas, 179
backbone routers, 179
benefits, 180
interarea routes, 179
internal routers, 179
intra-area routes, 179
MPLS VPNs, 361-362
network size, 178
problems, 177, 268
single-area, 177
SPF workload, reducing, 179
three-area, 178
best routes with SPF, calculating, 176-177
configuration
errors, troubleshooting, 269-270
mode, enabling, 186
default routes, 200-202
Dijkstra SPF algorithm, 170
EIGRP, compared, 214
goals, 287
Hello/dead timers, 279-280
history, 585
interarea routes, verifying, 199-200
interfaces
costs, setting, 202-204
EIGRP interfaces, compared, 268
identifying, 262
passive, 185
troubleshooting, 268-270
load balancing, 204
LSAs, 169
metrics, 202
based on interface bandwidth, 202-203
higher reference bandwidth, 204
setting, 204
MTU mismatched settings, 281
neighbors, 170-171
area mismatches, finding, 276-277
DRs on Ethernet links, 174-175
duplicate RIDs, 277-279
Hello messages, 171-172
Hello/dead timer mismatches, 279-280
LSAs, exchanging, 173
maintaining, 174
meeting, 171
neighbor requirements, 271
requirements, 275
RIDs, learning, 171
states, 172, 175, 275
troubleshooting, 274-280
process-ids, 186
processes, shutting down, 280-281
RIDs
configuring, 191-192
duplicate, troubleshooting, 277-279
super backbone, 361
Version 2. *See* OSPFv2
OSPFv2 (OSPF Version 2), 162
default routes, 200-202
dual stack, 585
interface configuration, 205-207
history, 585
load balancing, 204
metrics, 202
based on interface bandwidth, 202-203
higher reference bandwidth, 204
setting, 204
multiarea configuration, 194-197
network commands, 197
single-area configurations, 195-196
subnets, 194
verifying, 197-200

OSPFv3, compared, 587, 594
RIPv2/EIGRP, compared, 221
single-area configuration, 186-187
IPv4 addresses, 186
matching with network command, 187-188
multiarea configurations, 195-196
network command, 187
organization, 185
passive interfaces, 192-193
RIDs, 191-192
verifying, 188-190
wildcard masks, 187-188
OSPFv3 (OSPF Version 3), 584
address families dual stack, 586
configuration, 587
default routes, 593
load balancing, 592
multiarea example, 588
multiarea on ABR, 590-591
route selection metrics, setting, 592
single-area, 589-590
dual stack, 585
interfaces, 595
troubleshooting, 596-597
verifying, 595-596
IPv6
MTU mismatches, 601-602
routes, 602-605
LSAs, 600
LSDBs, 600-601
neighbors, 597
requirements, 598
troubleshooting, 598-600
verifying, 597-598
OSPFv2, compared, 587, 594
passive interfaces, 589
RIDs, 589
output queuing, 477
overages (MetroE data usage), 355-356
overlapping routes, troubleshooting, 545-548
overlapping subnets
with VLSM, 550-552
without VLSM, 549-550

P

PaaS (Platform as a Service), 706-707
packets
classification, 469
ACLs, 471
with marking, 470
matching, 470
NBAR, 471-472
router queuing, 469-470
routers, 471
congestion
avoidance, 484-485
management, 477-479
de-encapsulating/re-encapsulating with HDLC, 320
defined, 469
filtering. *See* ACLs
ICMPv6, 641
marking, 472
802.1Q headers, 473-474
802.11 headers, 474
with classification, 470
DiffServ DSCP values, 475-476
IP headers, 472-474
MPLS Label headers, 474
trust boundaries, 474
matching, 418
policing, 480-482
router originated, 637
router queuing, 469
routing over serial links, 376
shaping, 480-484
TCP, 641
UDP, 641
PAgP (Port Aggregation Protocol), 79
PAP (Password Authentication Protocol)
authentication, 326, 337-338
configuring, 328-330

parameters
ICMPv6, 635
ip_address, 187
wildcard_mask, 187
partial mesh topology (MetroE), 351
partial updates (EIGRP), 220, 223
passive-interface command, 193, 211, 284
EIGRP, 239, 259
OSPF, 185
OSPFv3, 589
passive-interface default command, 193, 259
passive interfaces
EIGRP, 239
OSPF, 185, 192-193
OSFPv3, 589
Password Authentication Protocol. *See* PAP
passwords, 664
path attributes (BGP), 289-290
Path MTU Discovery (PMTUD), 635
paths
forwarding, 738
selections, 163
PBX (private branch exchange), 29
PCP (Priority Code Point) field (802.1Q header), 473
PE (provider edge), 358
Pearson Network Simulator (the Sim), 758
peers, 287
periodic updates, 218
permit command, 445-447, 461
extended IPv6 ACLs, 640
GRE tunnel ACLs, 387
IPv6 ACLs, 638
permit gre command, 410
permit icmp any any router-advertisement command, 648
permit icmp any any router-solicitation command, 648
permit ipv6 commands, 653
permit keyword, 418, 424
per-VLAN Spanning Tree Plus (PVST+), 65-67
physical data center networks, 700
physical design (MetroE), 347-348
physical server model, 698
ping command, 455, 540-543, 583
IPv6
connectivity, testing, 570-571
routes, testing, 583
leased-line WANs, 335
self-ping, 456-457
ping6 command, 583
IPv6 ACLs, 639
IPv6 connectivity, testing, 570
pings (IPv6 hosts)
failure from default router, 574-575
name resolution problems, 575-576
working only in some cases, 573-574
planes (networking devices)
control, 726-727
data, 725-726
management, 727
Platform as a Service (PaaS), 706-707
PMTUD (Path MTU Discovery), 635
point-to-point edge ports, 56, 84
point-to-point GRE tunnels, 378
point-to-point lines. *See* leased-line WANs
Point-to-Point over Ethernet. *See* PPPoE
point-to-point ports, 56, 84
Point-to-Point Protocol. *See* PPP
Point-to-Point topology (MetroE), 349-350
points of presence (PoP), 288
policies
ACI, 735
filtering, 634
policing
data overages (MetroE), 355
QoS, 480
discarding excess traffic, 481
edge between networks, 481-482

features, *482*
traffic rate versus configured policing rate, *480-481*
rate, 480
pooling resources, 702
PoP (points of presence), 288, 347
Port Aggregation Protocol (PAgP), 79
PortChannels. *See* EtherChannels
PortFast, 57-58
configuring, 74
enabling/disabling, 75
global settings, displaying, 76
verifying, 75
ports
802.1w RSTP roles, 53
alternate, 53-54, 83
backup, 53, 83
blocking, choosing, 39
channels, 78
costs
IEEE default, *48*
STP, *46*, *71-72*
designated, 42, 47, 53
disabled, 53
Layer 3 switch routed, 505-508
numbers, matching, 438-441
per-VLAN STP costs, 68
root. *See* RPs
RSTP, 83
backup, *55*
roles, *53*
states, *84-85*
types, *56*, *84*
SPAN destination/source, 683
stacking ports, 147
states
RSTP, *84*
STP versus RSTP, *54*
switch root, choosing, 45-46
trusted/untrusted, 143-145
powers of 2 numeric reference table, 769
PPP (Point-to-Point Protocol), 323, 390
authentication, 325-326
CHAP
authentication, *325*, *337-338*
configuring, *327*
verifying, *328*
configuring, 326-327
control protocols, 324
dial connections to ISPs, 391
framing, 324
leased-line WANs, 323
multilink (MLPPP), 331
configuring, *332*
Layer 2 fragmentation balance, *331*
Layer 3, *331*
load balancing, *331*
verifying, *333-335*
PAP
authentication, *326*, *337-338*
configuring, *328-330*
PPPoE Layer 2 configuration, 393
status, 327
ppp authentication chap command, 327
ppp authentication command, 332, 343
ppp chap hostname command, 410
ppp chap password command, 410
ppp multilink command, 332, 344
ppp multilink group command, 344
ppp multilink group 1 command, 332
ppp pap sent-username command, 328, 343
PPPoE (Point-to-Point over Ethernet), 390-391
configuring, 392
ISP router configuration example, *395*
Layer 1, *393*
Layer 2, *393*
Layer 3, *394*
summary, *394-395*
enabling, 394
history, 391

troubleshooting, 401
customer router configuration, 401
dialer 2 status, 402
Layer 1, 402-403
Layer 2, 403-404
Layer 3, 404
summary, 405
verification, 396-397
dialers, 397-398
Layer 3 status, 400-401
session status, 399-400
virtual-access interfaces, 398
pppoe-client dial-pool number command, 393, 410
pppoe enable command, 394, 410
practice exams
answering questions, 753-755
CCNA R&S, 753
checklist, 753
ICND2, 753
knowledge gaps, finding, 755-756
other, 755
scores, 759
taking, 752-753
preemption (HSRP active/standby roles), 526-527
pre-exam suggestions, 750
prefixes
BGP, 288
IPv6, 564, 636
preparing for the exam
CLI skills, 757-758
exam-day suggestions, 750-751
knowledge gaps, finding, 755-756
practice exams
answering questions, 753-755
CCNA R&S, 753
checklist, 753
ICND2, 753
other, 755
scores, 759
taking, 752-753
pre-exam suggestions, 750
preparing for failure, 751-752
question types, 748
ready to pass assessment, 759
study tasks, 760
studying after failing to pass, 759-760
tutorial, 748-749
prioritization (congestion management), 477
Priority Code Point (PCP) field (802.1Q header), 473
priority queues, 478
priv keyword (snmp-server group command), 672
private branch exchange (PBX), 29
private cloud computing, 703-704
private WANs
MetroE, 347
access links, 348
data usage, 354-356
E-LAN services, 350-353
E-Line services, 349-353
E-Tree services, 351-354
full mesh topology, 350
hub and spoke topology, 351
IEEE Ethernet standards, 348
Layer 3 design, 352-354
MEF, 349
partial mesh topology, 351
physical design, 347-348
Point-to-Point topology, 349-350
services, 349
MPLS, 356-357
access links, 358
Layer 3 design, 358
VPNs EIGRP challenges, 360-363
QoS, 359-360
VPNs, 357
public cloud, accessing, 709-713
types, 346
probes, 677-678
process-ids (OSPF), 186

processes
OSPF, 280-281
RSTP, 55
programmability (network), 724
APIC Enterprise Module (APIC-EM), 735-737
Application Centric Infrastructure (ACI), 734-735
comparisons, 737
proprietary routing protocols, 166
protocols, 214
BGP, 165, 286
AS, 288
ASNs, 288
configuring, 293-297
IGPs, compared, 287
ISP default routes, learning, 303-304
neighbors, 287, 297
reachability, 287
route advertising, 287-288
routing table analysis reports website, 287
table entries, injecting, 298-303
update messages, 287, 294
BPDUs (bridge protocol data units), 43
CHAP
authentication, 325, 337-338
configuring, 327
verifying, 328
control plane, 727
DHCP
configuration settings, 144
DHCP-based attacks, 143-144
DHCP Binding Table, 145
features, 142
ports as trusted, configuring, 144
rate limiting, 145
rules summary, 144
trusted ports, 145
trusted/untrusted ports, 143
untrusted ports, 145
Dijkstra SPF algorithm, 170
DTP, 108
DV (distance vector), 166, 216
distance/vector information learned, 216-217
EIGRP as, 220-221
route poisoning, 219-220
split horizon, 219
update messages, 217-219
EAP, 138
EAPoL, 138
eBGP, 288-289
Internet edge, 290-293
neighbors, 294-297
EGP (exterior gateway protocol), 287
EIGRP. *See* EIGRP
FHRP, 516
features, 520
HSRP. See *Hot Standby Router Protocol (HSRP)*
need for, 519
options, 520
GLBP, 516
HDLC, 315, 319-323, 377
HSRP, 516, 521
active/passive model, 521
active/standby routers, choosing, 524
active/standby rules, 526
configuring, 523-524
failover, 521-522
group numbers, 524
load balancing, 522-523
with/without preemption, 526-527
troubleshooting, 528-531
verifying, 525
versions, 528
iBGP, 288-289
IGPs, 215
BGPs, compared, 287
configuring, 293
goals, 287
IGRP (Interior Gateway Routing Protocol), 166
IPv6, 585
link-state, 166

management plane, 727
matching, 437-438
MPBGP, 360
NDP, 563, 566
NHRP, 389
NTP, 718
OSPF. *See* OSPF
OSPFv2. *See* OSPFv2
OSPFv3. *See* OSPFv3
PAgP, 79
PAP
authentication, *326*, *337-338*
configuring, *328-330*
PPP. *See* PPP
PPPoE, 390-391
configuring, *392-395*
enabling, *394*
history, *391*
ISP router configuration example, *395*
troubleshooting, *401-405*
verification, *396-401*
RADIUS, 138-140
RIP, 166
RIPv2, 287
routable, 163
routed, 163
routing
administrative distance, *168*
algorithms, *165-166*
AS, *165*
autosummarization, *252-254*
classless/classful, *167*, *252*
convergence, *164*
defined, *163*
distance vector, *166*
DV. See *DV protocols*
EGP (exterior gateway protocol), *164*
functions, *163*
IGP, *164-167*
interfaces enabled with, *verifying*, *262*
interior comparison, *221*
IPv4, *190*
link-state, *166*
OSPF. See *OSPF*
path selections, *163*
proprietary, *166*
RIPv1, *215*
RIPv2, *215*
route redistribution, *167*
troubleshooting, *261-262*
RSTP, 51-52
alternate ports, *53-54*
backup port role, *55*
Cisco Catalyst STP modes, *80-82*
link types, *56*
port roles, *53*
port states, *54*
port types, *56*
processes, *55*
standards, *51*
STP, *compared*, *52*
RTP, 223
SNMP. *See* SNMP
STA (spanning-tree algorithm), 42
STP. *See* STP
TACACS+, 139-140
TCP
BPG connections, *displaying*, *296*
packets, *641*
port numbers, *matching*, *438-441*
transporting messages between BGP peers, *294*
windowing, *484-485*
UDP
Jitter probes, *677*
packets, *641*
port numbers, *matching*, *438-441*
VRRP, 516
VTP, 114
automated update powers, *114*
configuration, *121-122*
domains, *117-119*
features, *120*
planning configuration, *121*

pruning, *119-120*
requirements, *118-119*
servers, *116*
standard range VLANs, *116*
storing configuration, *125-126*
switches synchronization to VLAN database, *verifying*, *123-125*
synchronization, *117-118*
transparent mode, *126*
troubleshooting, *127-130*
versions, *119*
VLAN support, *adding*, *115*
provider edge (PE), 358
pruning (VTP), 119-120
public cloud computing, 704
accessing with
Internet, *707-709*
private WANs, *709-711*
VPNs, *709*
address assignment services, 717-718
branch offices example, 711-713
DHCP services, 718
DNS services, 716-717
intercloud exchanges, 710-711
NTP, 718-719
VNFs, 714-716
PVST+ (Per-VLAN Spanning Tree Plus), 65-67

Q

QoE (Quality of Experience), 466
QoS (Quality of Service), 359, 464
bandwidth, 465
classification, 469
ACLs, *471*
with marking, *470*
matching, *470*
NBAR, *471-472*
router queuing, *469-470*
routers, *471*
congestion
avoidance, *484-485*
management, *477-479*
defined, 464
delay, 465
jitter, 465
loss, 466
marking, 472
with classification, *470*
DiffServ DSCP values, *475-476*
Ethernet 802.1Q headers, *473-474*
Ethernet 802.11 headers, *474*
IP headers, *472-474*
MPLS Label headers, *474*
trust boundaries, *474*
MPLS, 359-360
needs based on traffic types
data, *466-467*
video, *468*
voice, *467-468*
policing, 480
discarding excess traffic, *481*
edge between networks, *481-482*
features, *482*
traffic rate versus configured policing rate, *480-481*
shaping, 480-483
features, *484*
slowing messages, *482*
time intervals, *483*
switches/routers, 469
tools, 469
VoIP, 467-468
query messages (EIGRP), 230
questions (exam)
answering, 753-755
budgeting time, 749
knowledge gaps, finding, 755-756
types, 748
queuing
congestion management, 477
Low Latency Queuing (LLQ), *478-479*
multiple queues, *477*

output queuing, 477
prioritization, 477
round robin scheduling, 477-478
strategy, 479
priority queues, 478
routers, classification for, 469
starvation, 479

R

RA (router advertisement) messages, 578, 648
RADIUS protocol, 138-140
rapid elasticity (cloud computing), 703
Rapid PVST+, 66
Rapid Spanning Tree Protocol. ***See*** **RSTP**
rate limiting (DHCP snooping), 145
RD (reported distance), 227-228, 244
reachability (BGP), 287
read-only (RO) communities (SNMP), 664
read-write (RW) communities (SNMP), 664
ready to pass assessment (exam), 759
Real-time Transport Protocol (RTP), 223
redistribution
Internet edge ISP routes, learning, 292
MPLS VPNs, 360
redundancy
FHRP, 519-520
LANs, 38-41
network needs for, 517-518
single points of failure, 517
reference bandwidth, 203-204
relationships (neighbors), 270
EIGRP for IPv6, 621-623
OSPFv3, troubleshooting, 598-600
pinging routers, confirming, 271
requirements, 271
states, 594
relay agents (DHCPv6), 566
Reliable Transport Protocol (RTP), 223
remark command, 445, 461
Remote SPAN (RSPAN), 684
reply messages (EIGRP), 230
reported distance (RD), 227-228, 244
Representational State Transfer (REST), 731
requirements
cloud computing services, 702
EIGRP for IPv6 neighbors, 621
neighbors, 271
EIGRP, 272
OSPF, 275
OSPFv3, 598
SNMPv3 configuration, 669
VTP, 118-119
resource pooling, 702
responders (IP SLAs), 677
REST (Representation State Transfer), 731
RESTful APIs, 731
reverse engineering from ACL to address range, 429-430
reversed source/destination IP address, troubleshooting, 452-453
RFC 1065, 661
RFC 4301, ***Security Architecture for the Internet Protocol*****, 374**
RIDs (router IDs), 171
defining, 185
EIGRP, configuring, 240
OSPF, 171
configuring, 191-192
duplicate, *troubleshooting*, 277-279
OSPFv3, 589
RIP (Routing Information Protocol), 166, 215
RIPv2 (RIP Version 2), 215
EIGRP/OSPFv2, compared, 221
goals, 287
RO (read-only) communities (SNMP), 664

ROAS (router-on-a-stick), 494-496
configuration, 496-498
troubleshooting, 500
verifying, 498-499
roles
ports
alternate, *53-54*
backup, *55*
root. See *RPs*
RSTP, *53*, *83*
STP, 50
root bridge IDs, 43
root costs (switches), 42
root ports. *See* RPs
root switches
electing, 44-45, 72-74
ruling out switches, 93-94
STP verification, 70
troubleshooting, 93-95
round robin scheduling (queuing), 477-478
round-trip delay, 465
Round Trip Time (RTT), 679
routable protocols, 163
routed ports, 506-508
routed protocols, 163
Router Advertisement (RA) messages, 578
router bgp command, 294-295
router eigrp command, 235, 258, 614
router-id command, 211
OSPFv3, 609, 589
RIDs, defining, 185
router-on-a-stick. *See* ROAS
router ospf command, 185, 211
router ospf 1 command, 186
Router Solicitation (RS), 578
routers. *See also* routes; routing
ABR (Area Border Router), 179
interface OSPF areas, *verifying*, *198*
OSPFv2 multiarea configuration, *196-197*
backbone, 179
best routes, finding, 170
classification, 471-472
Cloud Services Routers (CSRs), 709
configuring different VIPs, troubleshooting, 531
data plane processing, 725
designated (DRs), 174
backup (BDRs), *174*
discovering, *198-199*
Ethernet links, *174-175*
DROthers, 175
flooding, 169
GRE tunnels between, 377-378
HSRP
active/passive model, *521*
active/standby routers, *choosing*, *524*
active/standby rules, *526*
configuring, *523-524*
failover, *521-522*
group numbers, *524*
load balancing, *522-523*
with/without preemption, *526-527*
troubleshooting, *528-531*
verifying, *525*
versions, *528*
IDs. *See* RIDs
internal, 179, 589-590
IPv6
addressing configuration, *568*
connectivity, *verifying*, *571-572*
issues, *573*
routing, *enabling*, *567*
static route configuration, *568-569*
troubleshooting, *579-580*
ISP, 395
LSAs, 600
multiple serial links between, 330
OSPF interface costs, 202-204
public cloud networks, 715
QoS, 469

queuing
classification for, *469*
congestion management, *477-479*
strategy, *479*
redundant, 519. *See also* FHRP
ROAS, 494-496
configuration, *496-498*
native VLANs, *497-498*
subinterfaces, *creating*, *496-497*
troubleshooting, *500*
verifying, *498-499*
router WAN interface status, 552
routing IP packets over serial links, 376
troubleshooting
DHCP issues, *542-543*
LAN issues, *543-545*
VLAN routing, 17-18
routes. *See also* routers; routing
BGP, 287-290
classful networks, injecting, 298-300
default, 593
discard, 302
EIGRP
choosing, *222*
load balancing, *249-251*
tuning with bandwidth, *246*
variance, *250-251*
EIGRP for IPv6, 624-626
feasibility conditions, 229
feasible successor, 228-229
convergence, *247-248*
identifying, *245-247*
host, 339
interarea, 604
IPv6
EIGRP for IPv6 metrics, *616-617*
OSFPv3, *592*, *602-604*
static, *configuring*, *568-569*
troubleshooting, *604-605*
ISP
default, *learning*, *303-304*
Internet edge, *learning*, *292-293*
OSPF
default routes, *200-202*
interarea, *verifying*, *199-200*
poisoning, 219-220
redistribution, 360
static discard, 301-303
successor, 244-245
routing. *See also* routes; routers
EIGRP for IPv6, 616
LANs, 495
redistribution, 167
troubleshooting
default router IP address setting, *541*
DHCP issues, *542-543*
DNS problems, *540-541*
incorrect addressing plans, *549-552*
IP forwarding issues, *545-548*
LAN issues, *543-545*
mismatched IPv4 settings, *537-538*
mismatched masks, *538-539*
router WAN interface status, *552*
VLAN. *See* VLANs, routing
Routing Information Protocol (RIP), 166
routing protocols
administrative distance, 168
algorithms, 165-166
AS, 165
autosummarization, 252-254
classless/classful, 167, 252
convergence, 164
defined, 163
DV, 166, 216
distance/vector information learned, *216-217*
EIGRP as, *220-221*
route poisoning, *219-220*
split horizon, *219*
update messages, *217-219*
EGP (exterior gateway protocol), 164
functions, 163

IGP, 164
algorithms, 165-166
classless/classful, 167
metrics, 166-167
interfaces enabled with, verifying, 262
interior comparison, 221
IPv4, 190
link-state, 166
path selections, 163
proprietary, 166
RIPv1, 215
RIPv2, 215
route redistribution, 167
troubleshooting, 261-262
RPs (root ports)
nonroot switches, 94-96
switches, 45-46
RS (Router Solicitation) messages, 648
RSPAN (Remote SPAN), 684
RSTP (Rapid Spanning Tree Protocol), 51-52
alternate ports, 53-54
backup port role, 55
Cisco Catalyst switch RSTP modes, 80-82
implementing, 80
link types, 56
port roles, 53, 83
port states, 54, 84-85
port types, 56, 84
processes, 55
standards, 51
STP, compared, 52
RTP (Real-time Transport Protocol), 223
RTP (Reliable Transport Protocol), 223
RTT (Round Trip Time), 679
rules
AAA login authentication, 141-142
HSRP active/standby, 526
implicit IPv6 ACL ICMPv6 message filtering, 648-649
ruling out switches, 93-94
RW (read-write) communities (SNMP), 664

S

SaaS (Software as a Service), 706
SBIs (Southbound Interfaces), 729-730
scoring exams, 759
SDN (Software Defined Networking), 724
APIC Enterprise Module (APIC-EM), 735-737
Application Centric Infrastructure (ACI), 734-735
architecture, 732
comparisons, 737
controllers
centralized control, 729
Northbound Interfaces (NBIs), 730-732
OpenDaylight SDN controller, 733
Southbound Interfaces (SBIs), 729-730
Open SDN, 733
Open SDN Controller (OSC), 734
OpenDaylight (ODL), 733-734
OpenFlow, 732
sdm prefer command, 503
sdm prefer lanbase-routing command, 515
Secure Shell (SSH), 727
Secure Sockets Layer (SSL), 375-376
security
AAA servers
configuration, 140-141
login authentication rules, 141-142
login process, 139
TACACS+/RADIUS protocols, 139-140
access, 137
attacks, 142-144
authentication
802.1x, 137
AAA servers, 139-142

Internet VPNs, *373*
SNMPv3, *665*, *672-673*
DHCP snooping, 142-145
encryption, 665, 672-673
IEEE 802.1x, 137-138
Internet VPNs, 373
IPsec encryption, 374-375
SNMP, 664-665
SNMPv3, 669-671
STP, 58
self-ping, 456-457
sender's bridge IDs, 43
sender's root cost, 43
sequence numbers, 446-448
serial cables, 316
serial links. *See* leased-line WANs
servers
AAA
authentication, *139-142*
configuring for 802.1x, *137*
defining, *141*
enabling, *140*
username/passwords, *verifying*, *138*
Cisco hardware, 697
defined, 697
physical server model, 698
virtualization, 698-699
hosts, *699*
hypervisors, *699*
multithreading, *698*
networking, *700*
virtual data centers, *699-702*
VMs, *699*
VTP, 116
service-level agreements (SLAs), 676
service providers (SPs), 346
services
cloud computing
broad network access, *702*
cloud services catalogs, *703*
Infrastructure as a Service (IaaS), *705*
measured, *703*
on-demand self-service, *702*
Platform as a Service (PaaS), *706-707*
private, *703-704*
public, *704*
rapid elasticity, *703*
requirements, *702*
resource pooling, *702*
Software as a Service (SaaS), *706*
DHCP, 718
DNS, 716-717
Internet as WAN, 369
MetroE, 349
E-LAN, *350-353*
E-Line, *349-353*
E-Tree, *351-354*
public cloud
accessing, *707-711*
branch offices example, *711-713*
intercloud exchanges, *710-711*
public cloud address assignment, 717-718
session keys, 374
session status (PPPoE), 399-400
sessions (SPAN), 683-684, 687-688
Set messages
RO/RW communities, 664
SNMPv2 support, 665-666
writing variables on agents, 662
shaping (QoS), 480-483
features, 484
rate, 482
slowing messages, 482
time intervals, 483
shaping data overages (MetroE), 356
shared edge ports, 84
shared keys, 374
shared ports, 56, 84
shared session keys, 374
shorter VLAN configuration example, 23-24
Shortest Path First algorithm. *See* Dijkstra SPF algorithm
show access-list command, 446

show access-lists command, 425, 434, 452, 461, 653
show arp command, 541
show commands
IPv6 ACLs, 639
routing protocol-enabled interfaces, verifying, 262
STP status, 64
show controllers command, 334
show controllers serial command, 344
show etherchannel command, 90, 515
show etherchannel 1 summary command, 78
show etherchannel summary command, 100, 510
show interfaces command, 285, 344, 515, 538
EIGRP neighbor requirements, verifying, 272
MLPPP, 334
OSPF
interfaces, 270
neighbors, 275
OSPFv3 interface bandwidth, 604
PPP CHAP status, 328
PPP PAP, 329
PPP status, 327
routed ports, 507
show interfaces description command, 285, 545
show interfaces dialer command, 397, 410
show interfaces status command, 507, 510
show interfaces switchport command, 26-28, 31, 36, 106-108, 126
show interfaces trunk command, 26-28, 32, 36, 108
show interfaces tunnel command, 383, 410
show interfaces virtual-access command, 410
show interfaces virtual-access configuration command, 398
show interfaces vlan command, 515
show ip access-list command, 434, 447-449
show ip access-lists command, 425, 452, 461
show ip bgp command, 308
show ip bgp summary command, 296, 308
show ip eigrp interfaces command, 259, 284
EIGRP
enabled interfaces, 238-239, 262
neighbor requirements, verifying, 272
multilink interfaces, 333
show ip eigrp interfaces detail command, 238, 259
show ip eigrp neighbors command, 259, 284
neighbor status, displaying, 240
neighbor verification checks, 272
show ip eigrp topology command, 245, 259
feasible successor routes, 246
metrics, 248
topology table, 243
show ip eigrp topology all-links command, 247
show ip interface command, 426, 434, 451-452
show ip interface brief command, 344
GRE tunnels, 382
multilink interfaces, 333
OSPF interfaces, troubleshooting, 270
show ip interfaces command, 272
show ip ospf command, 211, 285
duplicate OSPF RIDs, 277
OSPF neighbors, troubleshooting, 275
show ip ospf database command, 169, 189, 212
show ip ospf interface command, 211, 285
DRs/BDRs details, displaying, 198
Hello/dead timer mismatches, 279
OSPF areas for ABR interfaces, 198
OSPF neighbors, troubleshooting, 275

OSPFv2 interface configuration, 207
passive interface, 193
show ip ospf interface brief command, 193, 211, 284
OSPF areas for ABR interfaces, 198
OSPF-enabled interfaces, identifying, 262
OSPF neighbors, troubleshooting, 275
OSPF status on interfaces, 268
OSPFv2 interface configuration, 207
show ip ospf neighbor command, 172, 211, 285
DRs/BDRs details, displaying, 198
neighbors, listing, 274
OSPF processes shutdown, 280
show ip ospf neighbor interface brief command, 280
show ip protocols command, 211, 259, 284
EIGRP-enabled interfaces, 239-240, 262
EIGRP neighbors, verifying, 241, 272
IPv4 routing protocols, 190
OSPF configuration errors, 269-270
OSPFv2 interface configuration, 206
show ip route command, 212, 259, 308, 546-548
administrative distance, 168
dialer interface Layer 3 orientation, 400
EIGRP-learned routes, displaying, 242
IPv4 routes added by OSPF, 190
routing tables, displaying, 515
show ip route eigrp command, 242, 259, 284
show ip route ospf command, 212, 285, 546
show ip route static command, 201
show ip sla enhanced-history distribution-statistics command, 694
show ip sla history command, 680, 694
show ip sla statistics command, 694
show ip sla summary command, 694
show ipv6 access-list commands, 653
show ipv6 access-lists command, 643
show ipv6 eigrp interfaces command, 620, 630
show ipv6 eigrp interfaces detail command, 630
show ipv6 eigrp neighbors command, 630
show ipv6 eigrp topology command, 631
show ipv6 eigrp topology | section command, 631
show ipv6 interface command, 583, 653
show ipv6 neighbors command, 583
IPv6 ACL ICMPv6 NDP message filtering, 646
IPv6 IPv4 replacement, 572
show ipv6 ospf command, 604, 610
show ipv6 ospf database command, 600, 610
show ipv6 ospf interface command, 595-596, 610
show ipv6 ospf interface brief command, 595, 604, 610
show ipv6 ospf neighbor command, 599, 610
show ipv6 protocols command, 583, 610
EIGRP for IPv6, 620, 630
OSPFv3 interfaces, 595
show ipv6 route command, 583, 610
EIGRP for IPv6, 631
IPv6 router connectivity, 572
show ipv6 route eigrp command, 631
show ipv6 route ospf command, 603, 610
show ipv6 route | section command, 631
show ipv6 routers command, 583, 646
show mac address-table command, 106
show mac address-table dynamic command, 103
show monitor detail command, 687, 694
show monitor session command, 687, 694
show monitor session all command, 686
show ppp all command, 328-329, 344
show ppp multilink command, 334, 344
show pppoe session command, 399, 410
show running-config command, 126, 424, 446-448

show snmp command, 668, 694
show snmp community command, 667, 694
show snmp contact command, 694
show snmp group command, 673, 694
show snmp host command, 667, 694
show snmp location command, 694
show snmp user command, 673, 694
show spanning-tree command, 90
show spanning-tree bridge command, 74
show spanning-tree interface command, 90
show spanning-tree interface detail command, 75
show spanning-tree root command, 70, 74
show spanning-tree summary command, 76, 90
show spanning-tree vlan command, 90
show spanning-tree vlan 10 command, 68, 70
show spanning-tree vlan 10 bridge command, 70
show spanning-tree vlan 10 interface gigabitethernet0/2 state command, 84
show standby command, 525, 529, 535
show standby brief command, 524, 535
show tcp brief command, 296
show tcp summary command, 308
show vlan command, 36, 106, 134
show vlan brief command, 21-24, 106
show vlan id command, 22, 106
show vlan status command, 126
show vlans command, 499, 515
show vtp password command, 126, 134
show vtp status command, 24, 36, 123, 126, 134
shutdown command, 36, 343
EIGRP for IPv6, 616, 630
Layer 1 leased-line WAN problems, 336
OSPF processes, 280
ROAS subinterfaces, 499
shutdown vlan command, 126, 134
shutting down OSPF processes, 280-281
signatures, 472
the Sim (Pearson Network Simulator), 758
Simple Network Management Protocol. ***See*** **SNMP**
single-area OSPF, 177
single-area OSPFv2 configuration, 186-187
IPv4 addresses, 186
matching with network command, 187-188
multiarea configurations, 195-196
network command, 187
organization, 185
passive interfaces, 192-193
RIDs, 191-192
verifying, 188-190
wildcard masks, 187-188
single-area OSPFv3 configuration, 589-590
single homed Internet edge design, 290
single points of failure, 517
site-to-site VPNs, 373-375
SLA (service level agreement), 676
SLAAC (stateless address autoconfiguration)
EUI-64, 567
IPv6 settings, 566-567
NDP, 566
troubleshooting, 577-578
SLBaaS (SLB as a service), 714
SNMP (Simple Network Management Protocol), 660
agents, 661
clear-text passwords, 664
communities, 664
Get messages
agent information, 662
RO/RW communities, 664
SNMPv2 configuration, 665-666
history, 661
Inform messages, 662-663, 666-667
managers, 661

MIB, 662-663
notifications, 662-663
read-only (RO) communities, 664
read-write (RW) communities, 664
security, 664-665
Set messages
RO/RW communities, *664*
SNMPv2 configuration, *665-666*
writing variables on agents, *662*
Trap messages, 662-663, 666-667
snmp-server command, 666
snmp-server community command, 693
snmp-server contact command, 693
snmp-server enable traps command, 693
snmp-server group command, 669-670
snmp-server host command, 666, 674, 693
snmp-server location command, 693
snmp-server user command, 671-672
SNMPv2
configuring
Get/Set messages, *665-666*
Trap/Inform messages, *666-667*
verifying, *667-669*
security, 664
SNMPv2c (Community-based SNMP Version 2), 664
SNMPv3
configuring, 669
authentication, *672-673*
encryption, *672-673*
groups, *669-671*
notifications, *674-675*
requirements, *669*
summary, *675-676*
users, *672*
verifying, *673*
groups, 670-671
Inform messages, 674-675
MIB views, 670
security, 664-665
Trap messages, 674-675
Software as a Service (SaaS), 706
Software Defined Networking. *See* SDN
solution apps, 738
sources
addresses, 384
IP SLAs, 677
IPs, matching, 437-438
SPAN, 683, 687-688
Southbound Interfaces (SBIs), 729-730
SPs (service providers), 346
SPAN (Switched Port Analyzer), 681
dependencies, 684-685
destination ports, 683
local, 684-687
network analyzer needs for, 682-683
Remote (RSPAN), 684
sessions, 683-684
source ports, 683
sources, limiting, 687-688
traffic direction, 687
VLANs, monitoring, 684
spanning-tree algorithm (STA), 42
spanning-tree bpduguard disable command, 89
spanning-tree bpduguard enable command, 74, 89
spanning-tree bpguard enable command, 68
spanning-tree commands, 89
spanning-tree mode command, 80, 89
spanning-tree mode mst command, 66
spanning-tree mode pvst command, 66
spanning-tree mode rapid-pvst command, 66, 82
spanning-tree pathcost method long command, 48
spanning-tree portfast command, 68, 74, 89
spanning-tree portfast bpduguard default command, 89
spanning-tree portfast default command, 75, 89
spanning-tree portfast disable command, 75, 89

Spanning Tree Protocol. *See* STP
spanning-tree vlan command, 67
spanning-tree vlan 10 port priority 112 command, 96
speed command, 545
speeds
LAN/WAN interfaces, 465
leased-line WANs, 317-318
SPF (Shortest Path First) algorithm, 170
Dijkstra SPF, 170
OSPF best routes, calculating, 176-177
spinning up VMs, 705
split horizon (DV routing protocols), 219
spoofing, 398
SSH (Secure Shell), 727
SSL (Secure Sockets Layer), 375-376
STA (spanning-tree algorithm), 42
stack masters, 148
stacking cables, 147
stacking modules, 147
stacking ports, 147
stacking switches
access layer switches, 147-148
benefits, 146
chassis aggregation, 149-151
FlexStack/FlexStack-Plus, 149
operating as single logical switch, 148
stack masters, 148
standard ACLs, configuring, 637-640
standard numbered IPv4 ACLs, 419
access-list command, 428-429
command syntax, 421
configuration examples, 424-427
list logic, 419-421
matching any/all addresses, 423-424
matching exact IP address, 421
matching subset of address, 421-423
overview, 419
reverse engineering from ACL to address range, 429-430
troubleshooting, 427-428
verification, 427-428
wildcard masks, 421-423
standard range VLANs, 116
standby 1 preempt command, 527
standby command, 523, 535
standby HSRP routers, 526
standby version command, 528
standby version 1 | 2 command, 535
stateful DHCP troubleshooting, 576-577
stateful DHCPv6, 565-566
stateless address autoconfiguration. *See* SLAAC
states
change reactions (STP topology), 49
discarding, 53
interfaces
changing with STP, 51
criteria, 42-43
forwarding/blocking, 41
learning, 51
listening, 51
neighbors, 172, 275
BGP, 297
OSPF, 175
OSPFv3, 597
relationships, 594
ports, 54, 84-85
ROAS subinterfaces, 498
STP, 50
tunnel interfaces, 384-385
VLAN mismatched trunking operational, 107-108
static discard routes, 301-303
static routes (IPv6), configuring, 568-569
status
BPDU Guard global settings, 76
EIGRP neighbors, 221, 240-241
HSRP, 525
interface codes, 335
PortFast global settings, 76
PPP, 327

PPP CHAP, 328
PPP PAP, 329
PPPoE, 399-401
STP, 68-70
steady-state operation (STP), 49
STP (Spanning Tree Protocol), 38
802.1D standard, 51
behind the scenes summary, 66
BIDs (bridge IDs), 43
root switch election, 44-45
system ID extensions, 67
BPDUs (bridge protocol data units), 43
BPDU Guard, 74-76
Cisco Catalyst switch STP modes, 80-81
configuration, 65
modes, 65-66
options, 68
per-VLAN port costs, 68
PVST+, 66-67
system ID extensions, 67
convergence, 42, 98
EtherChannels, 57
configuring, 76-79
MAC tables impact, predicting, 103-104
troubleshooting, 98-101
forwarding or blocking criteria, 42-43
interface states, changing, 51
LAN redundancy, 38-41
LAN segment DPs, choosing, 47
looping frames, preventing, 39
MAC tables impact, predicting, 102
PortFast, 57-58
configuring, 74
enabling/disabling, 75
global settings, displaying, 76
verifying, 75
ports
blocking, choosing, 39
costs, 46, 71-72
states, 54
purpose, 41-43
roles, 50
root election influence, 72-74
root switches, electing, 44-45, 93-94
RSTP. *See* RSTP
security, 58
STA (spanning-tree algorithm), 42
states, 50
steady-state operation, 49
switch reactions to changes, 49-50
switch RPs, choosing, 45-46
tiebreakers, 95-96
timers, 49-50
topology influences, 48-49
troubleshooting
convergence, 98
DPs on LAN segments, 96-98
root switch election, 93-95
RPs on nonroot switches, 94-96
verification, 68-70
studying after failing the exam, 759-760
studying for exam, 760
subinterfaces, 496-498
subnet masks
mismatched masks, 538-539
VLSM, 549-552
subnets
advertising to ISPs, 300-301
IGPs, 288
IPv6, 563-564
mismatched
EIGRP neighbors, 273
leased-line WANs, 339
OSPFv2 multiarea configuration, 194
overlapping subnets, 549-552
subset of IP address, matching, 421-423
successors
EIGRP, 228-229, 244-245
EIGRP for IPv6, 613
feasible
convergence, 247-248
identifying, 245-247
super backbone (OSPF), 361
superior Hello, 44

supplicants, 137
SVIs (switched virtual interfaces), 494, 501
configuring, 501-502
troubleshooting, 503-505
verifying, 502-503
Switched Port Analyzer. *See* SPAN
switches
as 802.1x authenticators, 137
access layer, 147-148
adding, 128-130
alternate ports, 53
backup ports, 53
BIDs (bridge IDs), 43
STP verification, 70
system ID extensions, 67
BPDUs (bridge protocol data units), 43
chassis aggregation, 149
benefits, 151
design, improving, 150
distribution/core switches high availability, 149-150
switch stacking, 149-151
Cisco Catalyst, 80-82
core, 149-150
data plane forwarding, analyzing, 102-104
distribution, 149-150
EtherChannel, 57
interfaces, 68
internal processing, 727-728
LAN segment DPs, choosing, 47
Layer 2 switches, 17
Layer 3 EtherChannels
configuring, 508-509
troubleshooting, 511
verifying, 510
Layer 3 with routed ports, 505-508
Layer 3 switches, 17-19
Layer 3 with SVIs
configuring, 501-502
troubleshooting, 503-505
verifying, 502-503
links, 56
logical, 148
nonroot, 94-96
PortFast, 57-58
ports
alternate role, 53-54
RSTP types, 56
QoS, 469
root
costs, 42
electing, 44-45, 72-74
ruling out switches, 93-94
STP verification, 70
troubleshooting, 93-95
RPs (root ports), choosing, 45-46
SPAN, 681
dependencies, 684-685
destination ports, 683
Encapsulated RSPAN (ERSPAN), 684
limiting sources, 687-688
local, 684-687
network analyzer needs, 682-683
Remote (RSPAN), 684
sessions, 683-684
source ports, 683
traffic direction, 687
VLANs, monitoring, 684
stacking
access layer switches, 147-148
benefits, 146
chassis aggregation, 149-151
FlexStack/FlexStack-Plus, 149
operating as single logical switch, 148
stack masters, 148
STP
changes, reacting, 49-50
topology influences, 48-49
synchronization to VLAN database, verifying, 123-125
ToR (Top of Rack), 700
traditional access switching, 146
virtual (vSwitches), 699

VLANs, enabling/disabling, 106
voice switches, 29
as VTP servers, 116
switchport access vlan command, 20, 23, 31, 36, 105, 126
switchport command, 506, 515
switchport mode command, 25, 36
switchport mode access command, 20, 23, 31, 130
switchport mode dynamic auto command, 107
switchport mode dynamic desirable command, 27
switchport mode trunk command, 24, 108, 496
switchport nonegotiate command, 28, 36, 108, 130
switchport trunk allowed vlan command, 36, 109
switchport trunk encapsulation command, 25, 36
switchport trunk native vlan command, 36, 110
switchport voice vlan command, 30-31, 36, 126
synchronizing
switches, 123-125
VTP, 117-118, 127-128
system ID extensions (BIDs), 67

T

T1. *See* leased-line WANs
T3, 318
TACACS+, 139-140
tagging (VLAN), 15
tail drops, 484
T-carrier systems, 317
TCAM (ternary content-addressable memory), 728
TCP (Transmission Control Protocol)
BGP connections, displaying, 296
packets, 641
port numbers, matching, 438-441
transporting messages between BGP peers, 294
windowing, 484-485
tcp keyword, 438
TCP/IP networks, 661
TDM (time-division multiplexing), 318
telcos (telephone companies), 315, 370
Telnet, 727
ternary content-addressable memory (TCAM), 728
testing IPv6
ACLs, 643
connectivity, 569-572
three-area OSPF, 178
TID fields (QoS marking), 474
tiebreakers (STP), 95-96
time (exam), 749-750
time burners, 749
time-division multiplexing (TDM), 318
time intervals (QoS shaping), 483
timers
EIGRP for IPv6, 618
EIGRP neighbors, 221
Hello messages, 174
Hello/dead mismatches, troubleshooting, 279-280
STP, 49-50
tools
APIC-EM Path Trace ACL Analysis tool, 738-739
APIC-EM Path Trace app, 738
QoS
ACLs, compared, 469
classification, 469-472
congestion avoidance, 484-485
congestion management, 477-479
marking, 472-476
policing, 480-482
queuing strategy, 479
shaping, 480-484
Top of Rack (ToR) switches, 700

topologies
EIGRP
displaying, *243-244*
feasible successor routes, *245-248*
metrics, *248*
successor routes, *identifying*, *244-245*
EIGRP for IPv6, 623-624
MetroE, 349-351
OSPF area design, 177
STP, influences, 48-49
ToR (Top of Rack) switches, 700
ToS (Type of Service) field (IPv4), 472
traceroute command, 543
GRE tunnels, 384
IPv6
connectivity, *testing*, *570-571*
network router problems, *troubleshooting*, *579*
routes, *testing*, *583*
traceroute6 command, 583
tracert command, 583
traditional access switching, 146
traffic
bandwidth, managing, 465
characteristics, 465
congestion
avoidance, *484-485*
management, *477-479*
delay, 465
end-user, 677
IPv6 ACLs, 636
jitter, 465
loss, 466
policing, 480
discarding excess traffic, *481*
edge between networks, *481-482*
features, *482*
traffic rate versus configured policing rate, *480-481*
public cloud branch office email services, 712-713
shaping, 480-483
SPAN sessions, 687
types
data, *466-467*
video, *468*
voice, *359*, *467-468*
Traffic Class field (IPv6), 473
Transmission Control Protocol. *See* TCP
transparent mode (VTP), 126
Trap messages, 662-663
SNMPv2, 666-667
SNMPv3, 674-675
troubleshooting
CHAP authentication failures, 337-338
DPs on LAN segments, 97
EIGRP interfaces, 263
configuration problems, *266-268*
working details, *264-266*
EIGRP for IPv6
interfaces, *621*
neighbors, *622-623*
routes, *625-626*
EIGRP neighbors, 273-274
EtherChannels, 98
channel-group command incorrect options, *98-100*
configuration checks before adding interfaces, *100-101*
GRE tunnels, 384
ACLs, *387-388*
interface state, *384-385*
Layer 3 issues, *386*
source/destination addresses, *384*
tunnel destination, *385-386*
HSRP, 528
ACL blocks HSRP packets, *531*
configuration, *529-530*
group number mismatches, *531*
misconfiguration symptoms, *530*
routers configuring different VIPs, *531*
version mismatches, *530-531*
with IP SLA, 679-681

IPv4 ACLs, 450
ACL behavior in network, 450-451
ACL interactions with router-generated packets, 455-457
common syntax mistakes, 453-454
inbound ACL filters routing protocol packets, 454-455
reversed source/destination IP address, 452-453
troubleshooting commands, 451-452
IPv4 routing
default router IP address setting, 541
DHCP issues, 542-543
DNS problems, 540-541
incorrect addressing plans, 549-552
IP forwarding issues, 545-548
LAN issues, 543-545
mismatched IPv4 settings, 537-538
mismatched masks, 538-539
packet filtering with access lists, 553
router WAN interface status, 552
IPv6 networks, 572
ACLs, 580
filtering issues, 573
host issues, 573
host pings fail from default router, 574-575
host pings only working in some cases, 573-574
missing IPv6 settings in host, 576-578
name resolution problems, 575-576
router issues, 573
routing, 579-580
IPv6 routes, 604-605
Layer 3 EtherChannels, 511
leased-line WANs, 335
Layer 1 problems, 335
Layer 2 problems, 336-338
Layer 3 problems, 338-339
mismatched subnets, 339
neighbors, 271
OSPF
interfaces, 268-270
MTU mismatched settings, 281
neighbors, 274-280
processes, shutting down, 280-281
OSPFv3
interfaces, 596-597
neighbors, 598-600
PAP authentication failures, 337-338
PPPoE, 401
customer router configuration, 401
dialer 2 status, 402
Layer 1, 402-403
Layer 2, 403-404
Layer 3, 404
summary, 405
ROAS, 500
routing protocols, 261-262
routing with SVIs, 503-505
RP problems, 96
SPAN sessions, 687-688
standard numbered ACLs, 427-428
STP
convergence, 98
DPs on LAN segments, 96-98
root switch election, 93-95
RPs on nonroot switches, 94-96
switch data plane forwarding
EtherChannel impact on MAC tables, 103-104
STP impact on MAC tables, 102
VLAN of incoming frames, 104-105
VLANs
access interfaces, 105-106
frame switching problems, 105
undefined/disabled VLANs, 106
VLAN trunking
frame switching problems, 105
mismatched native VLANs, 110
mismatched operational states, 107-108
mismatched supported VLAN lists, 108-109

VTP, 127
adding switches, *128-130*
common configuration rejections, *128*
synchronization, *127-128*
trunking (VLANs)
802.1Q, 16
configuration, 24-28
disabling, 130
ISL (Inter-Switch Link), 16
overview, 14
protocol. *See* VTP
VLAN tagging, 15
trust boundaries (QoS marking), 474
trusted ports, 143
configuring, 144
DHCP snooping, 145
tunnel destination command, 384-386, 409
tunnel mode gre ip command, 382, 410
tunnel mode gre multipoint command, 382
tunnel source command, 384, 409
tunnels
destinations, 385-386
GRE, 376
between routers, *377-378*
configuring, *380-382*
details, *displaying*, *382*
functionality, *testing*, *384*
large scale environments, *388*
multipoint with DMVPN, *389*
point-to-point, *378*
routes, *383*
troubleshooting, *384-388*
tunnel interfaces, *377*
unsecured networks, *378-380*
verifying, *382-384*
interfaces
ACLs, *387-388*
creating, *379*
destinations, *385-386*
Layer 3 issues, *386*
replacing serial links, *377*
state, *384-385*
VPN, 373-374
tutorial (exam), 748-749
Twitter (Wendell Odom), 761
Type of Service (ToS) field (IPv4), 472

U

UCS (Unified Computing System), 697
UDP (User Datagram Protocol)
Jitter probes, 677
packets, 641
port numbers, matching, 438-441
undebug all command, 285
undefined VLANs, troubleshooting, 106
unequal-cost load balancing, 250
UNI (user network interface), 348
unicast IPv6 addresses, 563-565
Unified Computing System (UCS), 697
unique local unicast addresses, 563
unsecured networks (GRE tunnels), 378-380
unsolicited log messages, 270
untrusted ports, 143-145
upd keyword, 438
updates
BGP, 287, 294
DV protocols, 217-219
EIGRP, 223-224
full, 218
partial, 220
periodic, 218
User Datagram Protocol. *See* UDP
user network interface (UNI), 348
username command, 327, 343
U.S. National Institute of Standards and Technology (NIST), 702

V

v1default MIB view, 670
variables (MIB), 662-663

variance (EIGRP), 250-251
variance command, 258
EIGRP, 235, 250, 614
EIGRP for IPv6, 618, 630
vCPU (virtual CPU), 698
vector (DV protocols), 216-217
verification command, 68
verifying
BPDU Guard, 75
data and voice VLANs, 30-32
eBGP neighbors, 296-297
EIGRP configuration, 237
EIGRP enabled interfaces, *finding*, *238-240*
IPv4 routing table, *displaying*, *241-242*
neighbors, *222*, *240-241*, *272-273*
EIGRP for IPv6
interfaces, *620*
routes, *624-625*
EtherChannel configuration before adding interfaces, 100-101
GRE tunnels, 382-384
HDLC, 322
HSRP, 525
interarea OSPF routes, 199-200
IPv6 connectivity, 569
hosts, *569-570*
routers, *571-572*
Layer 3 EtherChannels, 510
MLPPP, 333-335
OSPFv2 configuration
interface, *206-207*
multiarea, *197-200*
single-area, *188-190*
OSPFv3
interfaces, *595-596*, *602-604*
neighbors, *597-598*
PortFast, 75
PPP, 328-329
PPPoE, 396-397
dialers, *397-398*
Layer 3 status, *400-401*
session status, *399-400*
virtual-access interfaces, *398*
ROAS, 498-499
routing protocol-enabled interfaces, 262
routing with SVIs, 502-503
SNMPv2 configuration, 667-669
SNMPv3 configuration, 673
standard numbered ACLs, 427-428
STP, 68-70
switches synchronization to VLAN database, 123-125
username/passwords on AAA servers, 138
versions
HSRP, 528
OSPF, 585
VTP, 119
video traffic
QoS requirements, 468
shaping time intervals, 483
views (MIB), 670
virtual-access interfaces, 398
virtual LANs. *See* VLANs
virtual machines. *See* VMs
virtual network functions (VNFs), 714-716
Virtual Private LAN Service (VPLS), 349
Virtual Private Networks. *See* VPNs
Virtual Private Wire Service (VPWS), 349
Virtual Router Redundancy Protocol (VRRP), 516
virtualization
ASA firewall (ASAv), 715
CPU (vCPU), 698
data centers
networking, *699*
physical networks, *700*
vendors, *699*
workflow, *701-702*
firewalls, 715
networking, 699-700, 716
NICs (vNICS), 699

routers, 715
servers, 698-700
switches (vSwitches), 699
VMs. *See* VMs
VLANs (virtual LANs)
configuration
data and voice VLANs, *30-32*
database, *VTP synchronization*, *117-118*
full VLAN configuration example, *20-23*
overview, *20*
shorter VLAN configuration example, *23-24*
trunking, *24-28*
database switches synchronization, verifying, 123-125
default VLANs, 20
enabling/disabling, 106
IDs, 14
incoming frames, choosing, 104-105
interfaces. *See* SVIs
IP telephony, 28
data and voice VLAN concepts, *29-30*
data and voice VLAN configuration and verification, *30-32*
summary, *32*
LAN support, adding, 115
mismatched native on trunks, 110
mismatched supported trunk lists, 108-109
native, 16, 497-498
overview, 13-14
routing, 16-17
Layer 3 EtherChannels, *508-511*
Layer 3 switching with SVIs, *19*, *501-505*
Layer 3 switch routed ports, *505-508*
ROAS, *496-500*
with routers, *17-18*
SPAN monitoring, 684
standard range, 116
tagging, 15
troubleshooting, 105-106
trunking
802.1Q, *16*
configuration, *24-28*
disabling, *130*
ISL (Inter-Switch Link), *16*
overview, *14*
troubleshooting, *105-110*
VLAN tagging, *15*
VTP, *24*
vlan 10 command, 115
vlan 200 command, 128
vlan command, 20, 31, 36, 126
VLAN Trunking Protocol (VTP), 24, 114
VLSM (variable length subnet masking)
overlapping subnets, 550-552
recognizing when VLSM is used, 549
VMs (virtual machines), 698-699
ACI, 735
IaaS, 705
networking, 700
PaaS, 706-707
SaaS, 706
spinning up, 705
virtual NICs (vNICs), 699
VNFs (virtual network functions), 714-716
vNICs (virtual NICs), 699
voice switches, 29
voice traffic
QoS requirements, 467-468
shaping time intervals, 483
VoIP, 359
VoIP (Voice over IP), 359, 467-468
VPLS (Virtual Private LAN Service), 349
VPNs (Virtual Private Networks)
client, 375-376
dynamic multipoint (DMVPN), 389
Internet, 369
benefits, *374*
security, *373*

MPLS VPNs (MPLS Virtual Private Networks), 357
EIGRP challenges, *362-363*
Layer 3, *360-363*
OSPF area design, *361-362*
public cloud, accessing, 709
site-to-site, 373-375
tunnels, 373-374
VPWS (Virtual Private Wire Service), 349
VRRP (Virtual Router Redundancy Protocol), 516
vSwitches (virtual switches), 699
VTP (VLAN Trunking Protocol), 24, 114
automated update powers, 114
configuration
common rejections, *troubleshooting*, *128*
default VTP settings, *121*
example, *122*
new VTP configuration settings, *122*
planning, *121*
steps, *121*
storing, *125-126*
domains, 117-119
features, 120
pruning, 119-120
requirements, 118-119
servers, 116
standard range VLANs, 116
switches synchronization to VLAN database, verifying, 123-125
synchronization, 117
transparent mode, 126
troubleshooting, 127
adding switches, *128-130*
common configuration rejections, *128*
synchronization, *127-128*
versions, 119
VLAN support, adding, 115
vtp commands, 125
vtp domain command, 126, 133
vtp mode command, 36, 126, 133
vtp mode off command, 24, 126
vtp mode transparent command, 24, 126
vtp password command, 126, 133
vtp pruning command, 126, 134
vtp version command, 133

W

WANs
Ethernet, 709
Frame Relay, 346
interface cards (WICs), 317
interface speeds, 465
Internet access, 369
Internet as WAN service, 369
leased-line, 315
building, *319*
CSU/DSUs, *318*
mismatched subnets, *339*
physical components, *316-317*
speeds, *317-318*
troubleshooting, *335-339*
leased-line with HDLC, 319
configuring HDLC, *321-323*
de-encapsulating/re-encapsulating IP packets, *320*
framing, *320*
leased-line with PPP
authentication, *325-326*
configuring PPP, *326-327*
configuring PPP CHAP, *327-328*
configuring PPP PAP, *328-330*
control protocols, *324*
framing, *324*
multilink. See *MLPPP*
PPP functions, *323*
MetroE, 347
access links, *348*
data usage, *354-356*
E-LAN service, *350-353*
E-Line service, *349-353*
E-Tree service, *351-354*

full mesh topology, *350*
hub and spoke topology, *351*
IEEE Ethernet standards, *348*
Layer 3 design, *352-354*
MEF, *349*
partial mesh topology, *351*
physical design, *347-348*
Point-to-Point topology, *349-350*
services, *349*
MPLS, 356-357
access links, *358*
Layer 3 design, *358*
MPLS VPNs, *360-363*
QoS, *359-360*
VPNs, *357*
private
public cloud access, *709-711*
public cloud branch office connections, *713*
types, *346*
public cloud connections
Internet as, *707-709*
private WANs, *709-711*
service providers (SPs), 346
wireless, 371-372
WC masks. *See* wildcard masks
websites
ARIN, 165
BGP routing table analysis reports, 287
CCNA (ICND2) Config Labs, 758
Cisco
ACI, *735*
DevNet, *737*
Feature Navigator, *503*
Prime management products, *661*
Eclipse IDE, 707
ETSI, 716
Google App Engine PaaS, 707
IANA, 165
ICMPv6 parameters, *635*
IPv6 multicast address space registry, *647*
ICMPv6 packets, 635
Jenkins continuous integration and automation tool, 707
MEF, 349
OpenDaylight SDN controller, 733
OpenFlow, 730
Pearson Network Simulator (the Sim), 758
Wendell Odom's SDN Skills, 737
Wireshark network analyzer, 681
weighting, 477
Wendell Odom's SDN Skills blog, 737
WICs (WAN interface cards), 317
wildcard_mask parameter (network command), 187
wildcard masks
binary wildcard masks, 423
decimal wildcard masks, 421-423
EIGRP configuration, 236-237
finding right wildcard mask, 423
OSPF single-area configuration, 187-188
wireless Internet, 372
wireless WANs, 371-372
Wireshark network analyzer, 681
workflow (virtualized data center), 701-702
working interfaces, 43
write views (SNMPv3 groups), 671