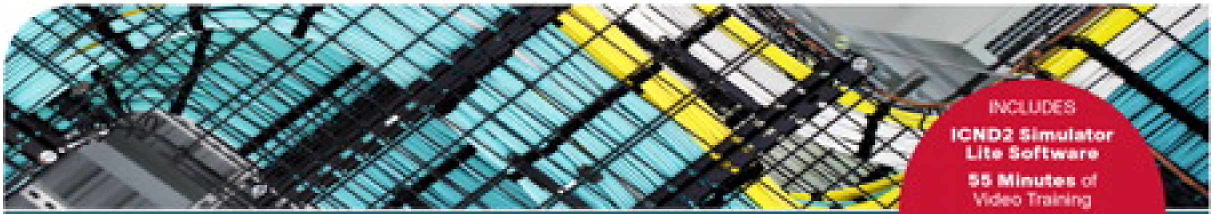
CISCO

Official Cert Guide

Learn, prepare, and practice for exam success



INCLUDES

ICND2 Simulator Lite Software

55 Minutes of Video Training

More than **300 Practice Exam Questions**

Online Practice Exercises

CCNA Routing and Switching ICND2 200-105

ciscopress.com

WENDELL ODOM, CCIE® NO. 1624

CCNA Routing and Switching
ICND2 200-105

Official Cert Guide

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

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 July 2016

Library of Congress Control Number: 2016936746

ISBN-13: 978-1-58720-579-8

ISBN-10: 1-58720-579-3

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 xxxv

Your Study Plan 2

Part I Ethernet LANs 13

Chapter 1 Implementing Ethernet Virtual LANs 14

Chapter 2 Spanning Tree Protocol Concepts 42

Chapter 3 Spanning Tree Protocol Implementation 68

Chapter 4 LAN Troubleshooting 98

Chapter 5 VLAN Trunking Protocol 120

Chapter 6 Miscellaneous LAN Topics 142

Part I Review 164

Part II IPv4 Routing Protocols 169

Chapter 7 Understanding OSPF Concepts 169

Chapter 8 Implementing OSPF for IPv4 194

Chapter 9 Understanding EIGRP Concepts 224

Chapter 10 Implementing EIGRP for IPv4 244

Chapter 11 Troubleshooting IPv4 Routing Protocols 272

Chapter 12 Implementing External BGP 300

Part II Review 324

Part III Wide-Area Networks 327

Chapter 13 Implementing Point-to-Point WANs 328

Chapter 14 Private WANs with Ethernet and MPLS 362

Chapter 15 Private WANs with Internet VPN 386

Part III Review 434

Part IV IPv4 Services: ACLs and QoS 437

Chapter 16 Basic IPv4 Access Control Lists 438

Chapter 17 Advanced IPv4 Access Control Lists 460

Chapter 18 Quality of Service (QoS) 488

Part IV Review 516

Part V IPv4 Routing and Troubleshooting 519

Chapter 19 IPv4 Routing in the LAN 520

Chapter 20 Implementing HSRP for First-Hop Routing 544

Chapter 21 Troubleshooting IPv4 Routing 566

Part V Review 588

Part VI IPv6 591

Chapter 22 IPv6 Routing Operation and Troubleshooting 592

Chapter 23 Implementing OSPF for IPv6 616

Chapter 24 Implementing EIGRP for IPv6 644

Chapter 25 IPv6 Access Control Lists 664

Part VI Review 688

Part VII Miscellaneous 691

Chapter 26 Network Management 692

Chapter 27 Cloud Computing 730

Chapter 28 SDN and Network Programmability 760

Part VII Review 780

Part VIII Final Prep 783

Chapter 29 Final Review 784

Part IX Appendixes 801

Appendix A Numeric Reference Tables 803

Appendix B Technical Content 810

Glossary 813

Index 852

DVD Appendixes

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

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 xxxv

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 5

Step 4: Use the Final Review Chapter to Refine Skills and Uncover Weaknesses 6

Step 5: Set Goals and Track Your Progress 7

Things to Do Before Starting the First Chapter 8

Find Review Activities on the Web and DVD 8

Should I Plan to Use the Two-Exam Path or One-Exam Path? 8

Study Options for Those Taking the 200-125 CCNA Exam 9

Other Small Tasks Before Getting Started 10

Getting Started: Now 11

Part I Ethernet LANs 13

Chapter 1 Implementing Ethernet Virtual LANs 14

"Do I Know This Already?" Quiz 14

Foundation Topics 16

Virtual LAN Concepts 16

Creating Multiswitch VLANs Using Trunking 18

VLAN Tagging Concepts 18

The 802.1Q and ISL VLAN Trunking Protocols 20

Forwarding Data Between VLANs 21

Routing Packets Between VLANs with a Router 21

Routing Packets with a Layer 3 Switch 23

VLAN and VLAN Trunking Configuration and Verification 24

Creating VLANs and Assigning Access VLANs to an Interface 24

VLAN Configuration Example 1: Full VLAN Configuration 25

VLAN Configuration Example 2: Shorter VLAN Configuration 28

VLAN Trunking Protocol 29

VLAN Trunking Configuration 30

Implementing Interfaces Connected to Phones 34

Data and Voice VLAN Concepts 34

Data and Voice VLAN Configuration and Verification 36

Summary: IP Telephony Ports on Switches 38

Chapter Review 39

Chapter 2 Spanning Tree Protocol Concepts 42

"Do I Know This Already?" Quiz 43

Foundation Topics 44

Spanning Tree Protocol (IEEE 802.1D) 44

The Need for Spanning Tree 45

What IEEE 802.1D Spanning Tree Does 47

How Spanning Tree Works 48

The STP Bridge ID and Hello BPDU 49

Electing the Root Switch 50

Choosing Each Switch's Root Port 52

Choosing the Designated Port on Each LAN Segment 54

Influencing and Changing the STP Topology 54

Making Configuration Changes to Influence the STP Topology 55

Reacting to State Changes That Affect the STP Topology 55

How Switches React to Changes with STP 56

Changing Interface States with STP 57

Rapid STP (IEEE 802.1w) Concepts 58

Comparing STP and RSTP 59

RSTP and the Alternate (Root) Port Role 60

RSTP States and Processes 62

RSTP and the Backup (Designated) Port Role 62

RSTP Port Types 63

Optional STP Features 64

EtherChannel 64

PortFast 65

BPDU Guard 65

Chapter Review 66

Chapter 3 Spanning Tree Protocol Implementation 68

"Do I Know This Already?" Quiz 69

Foundation Topics 71

Implementing STP 71

Setting the STP Mode 72
Connecting STP Concepts to STP Configuration Options 72
Per-VLAN Configuration Settings 72
The Bridge ID and System ID Extension 73
Per-VLAN Port Costs 74
STP Configuration Option Summary 74
Verifying STP Operation 75
Configuring STP Port Costs 78
Configuring Priority to Influence the Root Election 80
Implementing Optional STP Features 81
Configuring PortFast and BPDU Guard 81
Configuring EtherChannel 84
Configuring a Manual EtherChannel 84
Configuring Dynamic EtherChannels 86
Implementing RSTP 88
Identifying the STP Mode on a Catalyst Switch 88
RSTP Port Roles 91
RSTP Port States 92
RSTP Port Types 92
Chapter Review 94

Chapter 4 LAN Troubleshooting 98

"Do I Know This Already?" Quiz 99
Foundation Topics 99
Troubleshooting STP 99
Determining the Root Switch 99
Determining the Root Port on Nonroot Switches 101
STP Tiebreakers When Choosing the Root Port 102
Suggestions for Attacking Root Port Problems on the Exam 103
Determining the Designated Port on Each LAN Segment 104
Suggestions for Attacking Designated Port Problems on the Exam 105
STP Convergence 105
Troubleshooting Layer 2 EtherChannel 106
Incorrect Options on the channel-group Command 106
Configuration Checks Before Adding Interfaces to EtherChannels 108

Analyzing the Switch Data Plane Forwarding 109
Predicting STP Impact on MAC Tables 110
Predicting EtherChannel Impact on MAC Tables 111
Choosing the VLAN of Incoming Frames 112
Troubleshooting VLANs and VLAN Trunks 113
Access VLAN Configuration Incorrect 113
Access VLANs Undefined or Disabled 114
Mismatched Trunking Operational States 116
Mismatched Supported VLAN List on Trunks 117
Mismatched Native VLAN on a Trunk 118
Chapter Review 119

Chapter 5 VLAN Trunking Protocol 120
"Do I Know This Already?" Quiz 120
Foundation Topics 122
VLAN Trunking Protocol (VTP) Concepts 122
Basic VTP Operation 122
Synchronizing the VTP Database 124
Requirements for VTP to Work Between Two Switches 126
VTP Version 1 Versus Version 2 127
VTP Pruning 127
Summary of VTP Features 128
VTP Configuration and Verification 129
Using VTP: Configuring Servers and Clients 129
Verifying Switches Synchronized Databases 131
Storing the VTP and Related Configuration 134
Avoiding Using VTP 135
VTP Troubleshooting 135
Determining Why VTP Is Not Synchronizing 136
Common Rejections When Configuring VTP 137
Problems When Adding Switches to a Network 137
Chapter Review 139

Chapter 6 Miscellaneous LAN Topics 142
"Do I Know This Already?" Quiz 143
Foundation Topics 144
Securing Access with IEEE 802.1x 144

AAA Authentication 147

AAA Login Process 147

TACACS+ and RADIUS Protocols 147

AAA Configuration Examples 148

DHCP Snooping 150

DHCP Snooping Basics 151

An Example DHCP-based Attack 152

How DHCP Snooping Works 152

Summarizing DHCP Snooping Features 154

Switch Stacking and Chassis Aggregation 155

Traditional Access Switching Without Stacking 155

Switch Stacking of Access Layer Switches 156

Switch Stack Operation as a Single Logical Switch 157

Cisco FlexStack and FlexStack-Plus 158

Chassis Aggregation 159

High Availability with a Distribution/Core Switch 159

Improving Design and Availability with Chassis Aggregation 160

Chapter Review 162

Part I Review 164

Part II IPv4 Routing Protocols 169

Chapter 7 Understanding OSPF Concepts 170

“Do I Know This Already?” Quiz 170

Foundation Topics 172

Comparing Dynamic Routing Protocol Features 172

Routing Protocol Functions 172

Interior and Exterior Routing Protocols 173

Comparing IGPs 175

IGP Routing Protocol Algorithms 175

Metrics 175

Other IGP Comparisons 176

Administrative Distance 177

OSPF Concepts and Operation 178

OSPF Overview 179

Topology Information and LSAs 179

Applying Dijkstra SPF Math to Find the Best Routes 180

Becoming OSPF Neighbors 180
The Basics of OSPF Neighbors 181
Meeting Neighbors and Learning Their Router ID 181
Exchanging the LSDB Between Neighbors 183
Fully Exchanging LSAs with Neighbors 183
Maintaining Neighbors and the LSDB 184
Using Designated Routers on Ethernet Links 185
Calculating the Best Routes with SPF 186
OSPF Area Design 188
OSPF Areas 189
How Areas Reduce SPF Calculation Time 190
OSPF Area Design Advantages 191
Chapter Review 191

Chapter 8 Implementing OSPF for IPv4 194

"Do I Know This Already?" Quiz 194
Foundation Topics 196
Implementing Single-Area OSPFv2 196
OSPF Single-Area Configuration 197
Matching with the OSPF network Command 198
Verifying OSPFv2 Single Area 200
Configuring the OSPF Router ID 203
OSPF Passive Interfaces 204
Implementing Multiarea OSPFv2 206
Single-Area Configurations 207
Multiarea Configuration 209
Verifying the Multiarea Configuration 210
Verifying the Correct Areas on Each Interface on an ABR 210
Verifying Which Router Is DR and BDR 211
Verifying Interarea OSPF Routes 212
Additional OSPF Features 213
OSPF Default Routes 213
OSPF Metrics (Cost) 215
Setting the Cost Based on Interface Bandwidth 216
The Need for a Higher Reference Bandwidth 217
OSPF Load Balancing 217

OSPFv2 Interface Configuration 218
OSPFv2 Interface Configuration Example 218
Verifying OSPFv2 Interface Configuration 219
Chapter Review 221
Chapter 9 Understanding EIGRP Concepts 224
"Do I Know This Already?" Quiz 224
Foundation Topics 226
EIGRP and Distance Vector Routing Protocols 226
Introduction to EIGRP 226
Basic Distance Vector Routing Protocol Features 227
The Concept of a Distance and a Vector 228
Full Update Messages and Split Horizon 229
Route Poisoning 231
EIGRP as an Advanced DV Protocol 232
EIGRP Sends Partial Update Messages, As Needed 232
EIGRP Maintains Neighbor Status Using Hello 233
Summary of Interior Routing Protocol Features 233
EIGRP Concepts and Operation 234
EIGRP Neighbors 234
Exchanging EIGRP Topology Information 235
Calculating the Best Routes for the Routing Table 236
The EIGRP Metric Calculation 236
An Example of Calculated EIGRP Metrics 237
Caveats with Bandwidth on Serial Links 238
EIGRP Convergence 239
Feasible Distance and Reported Distance 240
EIGRP Successors and Feasible Successors 241
The Query and Reply Process 242
Chapter Review 243
Chapter 10 Implementing EIGRP for IPv4 244
"Do I Know This Already?" Quiz 244
Foundation Topics 246
Core EIGRP Configuration and Verification 246
EIGRP Configuration 246
Configuring EIGRP Using a Wildcard Mask 248

Verifying EIGRP Core Features 249
Finding the Interfaces on Which EIGRP Is Enabled 250
Displaying EIGRP Neighbor Status 253
Displaying the IPv4 Routing Table 253
EIGRP Metrics, Successors, and Feasible Successors 255
Viewing the EIGRP Topology Table 255
Finding Successor Routes 257
Finding Feasible Successor Routes 258
Convergence Using the Feasible Successor Route 260
Examining the Metric Components 262
Other EIGRP Configuration Settings 262
Load Balancing Across Multiple EIGRP Routes 263
Tuning the EIGRP Metric Calculation 265
Autosummarization and Discontiguous Classful Networks 266
Automatic Summarization at the Boundary of a Classful Network 266
Discontiguous Classful Networks 267
Chapter Review 269

Chapter 11 Troubleshooting IPv4 Routing Protocols 272
"Do I Know This Already?" Quiz 272
Foundation Topics 273
Perspectives on Troubleshooting Routing Protocol Problems 273
Interfaces Enabled with a Routing Protocol 274
EIGRP Interface Troubleshooting 275
Examining Working EIGRP Interfaces 276
Examining the Problems with EIGRP Interfaces 278
OSPF Interface Troubleshooting 281
Neighbor Relationships 284
EIGRP Neighbor Verification Checks 285
EIGRP Neighbor Troubleshooting Example 286
OSPF Neighbor Troubleshooting 288
Finding Area Mismatches 290
Finding Duplicate OSPF Router IDs 291
Finding OSPF Hello and Dead Timer Mismatches 293
Other OSPF Issues 294
Shutting Down the OSPF Process 294
Mismatched MTU Settings 296
Chapter Review 296

Chapter 12 Implementing External BGP 300

"Do I Know This Already?" Quiz 300

Foundation Topics 302

BGP Concepts 302

Advertising Routes with BGP 303

Internal and External BGP 304

Choosing the Best Routes with BGP 305

eBGP and the Internet Edge 306

Internet Edge Designs and Terminology 306

Advertising the Enterprise Public Prefix into the Internet 307

Learning Default Routes from the ISP 309

eBGP Configuration and Verification 309

BGP Configuration Concepts 310

Configuring eBGP Neighbors Using Link Addresses 311

Verifying eBGP Neighbors 312

Administratively Disabling Neighbors 314

Injecting BGP Table Entries with the network Command 314

Injecting Routes for a Classful Network 315

Advertising Subnets to the ISP 318

Advertising a Single Prefix with a Static Discard Route 319

Learning a Default Route from the ISP 320

Chapter Review 321

Part II Review 324

Part III Wide-Area Networks 327

Chapter 13 Implementing Point-to-Point WANs 328

"Do I Know This Already?" Quiz 328

Foundation Topics 330

Leased-Line WANs with HDLC 330

Layer 1 Leased Lines 331

The Physical Components of a Leased Line 332

The Role of the CSU/DSU 334

Building a WAN Link in a Lab 335

Layer 2 Leased Lines with HDLC 336

Configuring HDLC 337

Leased-Line WANs with PPP 340

PPP Concepts 340

PPP Framing 341

PPP Control Protocols 341

PPP Authentication 342

Implementing PPP 343

Implementing PPP CHAP 344

Implementing PPP PAP 346

Implementing Multilink PPP 347

Multilink PPP Concepts 348

Configuring MLPPP 349

Verifying MLPPP 351

Troubleshooting Serial Links 353

Troubleshooting Layer 1 Problems 354

Troubleshooting Layer 2 Problems 354

Keepalive Failure 355

PAP and CHAP Authentication Failure 356

Troubleshooting Layer 3 Problems 357

Chapter Review 358

Chapter 14 Private WANs with Ethernet and MPLS 362

"Do I Know This Already?" Quiz 363

Foundation Topics 364

Metro Ethernet 364

Metro Ethernet Physical Design and Topology 365

Ethernet WAN Services and Topologies 366

Ethernet Line Service (Point-to-Point) 367

Ethernet LAN Service (Full Mesh) 368

Ethernet Tree Service (Hub and Spoke) 369

Layer 3 Design Using Metro Ethernet 370

Layer 3 Design with E-Line Service 370

Layer 3 Design with E-LAN Service 371

Layer 3 Design with E-Tree Service 372

Ethernet Virtual Circuit Bandwidth Profiles 373

Charging for the Data (Bandwidth) Used 373

Controlling Overages with Policing and Shaping 374

Multiprotocol Label Switching (MPLS) 375
MPLS VPN Physical Design and Topology 377
MPLS and Quality of Service 378
Layer 3 with MPLS VPN 379
OSPF Area Design with MPLS VPN 381
Routing Protocol Challenges with EIGRP 382
Chapter Review 383

Chapter 15 Private WANs with Internet VPN 386

"Do I Know This Already?" Quiz 386
Foundation Topics 389
Internet Access and Internet VPN Fundamentals 389
Internet Access 389
Digital Subscriber Line 390
Cable Internet 391
Wireless WAN (3G, 4G, LTE) 392
Fiber Internet Access 393
Internet VPN Fundamentals 393
Site-to-Site VPNs with IPsec 395
Client VPNs with SSL 396
GRE Tunnels and DMVPN 397
GRE Tunnel Concepts 398
Routing over GRE Tunnels 398
GRE Tunnels over the Unsecured Network 400
Configuring GRE Tunnels 402
Verifying a GRE Tunnel 404
Troubleshooting GRE Tunnels 406
Tunnel Interfaces and Interface State 406
Layer 3 Issues for Tunnel Interfaces 409
Issues with ACLs and Security 409
Multipoint Internet VPNs Using DMVPN 410
PPP over Ethernet 413
PPPoE Concepts 414
PPPoE Configuration 415
PPPoE Configuration Breakdown: Dialers and Layer 1 416
PPPoE Configuration Breakdown: PPP and Layer 2 417
PPPoE Configuration Breakdown: Layer 3 417

PPPoE Configuration Summary 418

A Brief Aside About Lab Experimentation with PPPoE 419

PPPoE Verification 420

Verifying Dialer and Virtual-Access Interface Bindings 421

Verifying Virtual-Access Interface Configuration 422

Verifying PPPoE Session Status 424

Verifying Dialer Interface Layer 3 Status 425

PPPoE Troubleshooting 425

Step 0: Status Before Beginning the First Step 426

Step 1: Status After Layer 1 Configuration 427

Step 2: Status After Layer 2 (PPP) Configuration 428

Step 3: Status After Layer 3 (IP) Configuration 429

PPPoE Troubleshooting Summary 430

Chapter Review 430

Part III Review 434

Part IV IPv4 Services: ACLs and QoS 437

Chapter 16 Basic IPv4 Access Control Lists 438

"Do I Know This Already?" Quiz 438

Foundation Topics 440

IPv4 Access Control List Basics 440

ACL Location and Direction 440

Matching Packets 441

Taking Action When a Match Occurs 442

Types of IP ACLs 442

Standard Numbered IPv4 ACLs 443

List Logic with IP ACLs 444

Matching Logic and Command Syntax 445

Matching the Exact IP Address 445

Matching a Subset of the Address with Wildcards 446

Binary Wildcard Masks 447

Finding the Right Wildcard Mask to Match a Subnet 448

Matching Any/All Addresses 448

Implementing Standard IP ACLs 448

Standard Numbered ACL Example 1 449

Standard Numbered ACL Example 2 450

Troubleshooting and Verification Tips 452

Practice Applying Standard IP ACLs 453
Practice Building access-list Commands 454
Reverse Engineering from ACL to Address Range 454
Chapter Review 456
Chapter 17 Advanced IPv4 Access Control Lists 460
“Do I Know This Already?” Quiz 461
Foundation Topics 462
Extended Numbered IP Access Control Lists 462
Matching the Protocol, Source IP, and Destination IP 463
Matching TCP and UDP Port Numbers 464
Extended IP ACL Configuration 467
Extended IP Access Lists: Example 1 468
Extended IP Access Lists: Example 2 469
Practice Building access-list Commands 470
Named ACLs and ACL Editing 471
Named IP Access Lists 471
Editing ACLs Using Sequence Numbers 473
Numbered ACL Configuration Versus Named ACL Configuration 475
ACL Implementation Considerations 476
Troubleshooting with IPv4 ACLs 477
Analyzing ACL Behavior in a Network 477
ACL Troubleshooting Commands 479
Example Issue: Reversed Source/Destination IP Addresses 480
Steps 3D and 3E: Common Syntax Mistakes 481
Example Issue: Inbound ACL Filters Routing Protocol Packets 481
ACL Interactions with Router-Generated Packets 483
Local ACLs and a Ping from a Router 483
Router Self-Ping of a Serial Interface IPv4 Address 483
Router Self-Ping of an Ethernet Interface IPv4 Address 484
Chapter Review 485
Chapter 18 Quality of Service (QoS) 488
“Do I Know This Already?” Quiz 488
Foundation Topics 490
Introduction to QoS 490
QoS: Managing Bandwidth, Delay, Jitter, and Loss 491
Types of Traffic 492
Data Applications 492
Voice and Video Applications 493

QoS as Mentioned in This Book 495

QoS on Switches and Routers 495

Classification and Marking 495

Classification Basics 495

Matching (Classification) Basics 496

Classification on Routers with ACLs and NBAR 497

Marking IP DSCP and Ethernet CoS 499

Marking the IP Header 499

Marking the Ethernet 802.1Q Header 500

Other Marking Fields 501

Defining Trust Boundaries 501

DiffServ Suggested Marking Values 502

Expedited Forwarding (EF) 502

Assured Forwarding (AF) 502

Class Selector (CS) 503

Congestion Management (Queuing) 504

Round Robin Scheduling (Prioritization) 505

Low Latency Queuing 505

A Prioritization Strategy for Data, Voice, and Video 507

Shaping and Policing 507

Policing 508

Where to Use Policing 509

Shaping 510

Setting a Good Shaping Time Interval for Voice and Video 511

Congestion Avoidance 512

TCP Windowing Basics 512

Congestion Avoidance Tools 513

Chapter Review 514

Part IV Review 516

Part V IPv4 Routing and Troubleshooting 519

Chapter 19 IPv4 Routing in the LAN 520

“Do I Know This Already?” Quiz 521

Foundation Topics 522

VLAN Routing with Router 802.1Q Trunks 522

Configuring ROAS 524

Verifying ROAS 526

Troubleshooting ROAS 528

VLAN Routing with Layer 3 Switch SVIs 529

Configuring Routing Using Switch SVIs 529

Verifying Routing with SVIs 531

Troubleshooting Routing with SVIs 532

VLAN Routing with Layer 3 Switch Routed Ports 534

Implementing Routed Interfaces on Switches 535

Implementing Layer 3 EtherChannels 537

Troubleshooting Layer 3 EtherChannels 541

Chapter Review 541

Chapter 20 Implementing HSRP for First-Hop Routing 544

"Do I Know This Already?" Quiz 544

Foundation Topics 546

FHRP and HSRP Concepts 546

The Need for Redundancy in Networks 547

The Need for a First Hop Redundancy Protocol 549

The Three Solutions for First-Hop Redundancy 550

HSRP Concepts 551

HSRP Failover 552

HSRP Load Balancing 553

Implementing HSRP 554

Configuring and Verifying Basic HSRP 554

HSRP Active Role with Priority and Preemption 556

HSRP Versions 559

Troubleshooting HSRP 560

Checking HSRP Configuration 560

Symptoms of HSRP Misconfiguration 561

Chapter Review 563

Chapter 21 Troubleshooting IPv4 Routing 566

"Do I Know This Already?" Quiz 567

Foundation Topics 567

Problems Between the Host and the Default Router 567

Root Causes Based on a Host's IPv4 Settings 568

Ensure IPv4 Settings Correctly Match 568

Mismatched Masks Impact Route to Reach Subnet 569

Typical Root Causes of DNS Problems 571

Wrong Default Router IP Address Setting 572

Root Causes Based on the Default Router's Configuration 572
DHCP Issues 573
Router LAN Interface and LAN Issues 575
Problems with Routing Packets Between Routers 576
IP Forwarding by Matching the Most Specific Route 577
Using show ip route and Subnet Math to Find the Best Route 577
Using show ip route address to Find the Best Route 579
show ip route Reference 579
Routing Problems Caused by Incorrect Addressing Plans 581
Recognizing When VLSM Is Used or Not 581
Overlaps When Not Using VLSM 581
Overlaps When Using VLSM 583
Configuring Overlapping VLSM Subnets 584
Pointers to Related Troubleshooting Topics 585
Router WAN Interface Status 585
Filtering Packets with Access Lists 586
Chapter Review 586

Part V Review 588

Part VI IPv6 591

Chapter 22 IPv6 Routing Operation and Troubleshooting 592
"Do I Know This Already?" Quiz 592
Foundation Topics 592
Normal IPv6 Operation 592
Unicast IPv6 Addresses and IPv6 Subnetting 593
Assigning Addresses to Hosts 595
Stateful DHCPv6 596
Stateless Address Autoconfiguration 597
Router Address and Static Route Configuration 598
Configuring IPv6 Routing and Addresses on Routers 598
IPv6 Static Routes on Routers 599
Verifying IPv6 Connectivity 600
Verifying Connectivity from IPv6 Hosts 600
Verifying IPv6 from Routers 601
Troubleshooting IPv6 604
Pings from the Host Work Only in Some Cases 605
Pings Fail from a Host to Its Default Router 606

Problems Using Any Function That Requires DNS 607

Host Is Missing IPv6 Settings: Stateful DHCP Issues 608

Host Is Missing IPv6 Settings: SLAAC Issues 609

Traceroute Shows Some Hops, But Fails 610

Routing Looks Good, But Traceroute Still Fails 612

Chapter Review 612

Chapter 23 Implementing OSPF for IPv6 616

"Do I Know This Already?" Quiz 616

Foundation Topics 618

OSPFv3 for IPv6 Concepts 618

IPv6 Routing Protocol Versions and Protocols 619

Two Options for Implementing Dual Stack with OSPF 619

OSPFv2 and OSPFv3 Internals 621

OSPFv3 Configuration 621

Basic OSPFv3 Configuration 621

Single-Area Configuration on the Three Internal Routers 623

Adding Multiarea Configuration on the Area Border Router 625

Other OSPFv3 Configuration Settings 626

Setting OSPFv3 Interface Cost to Influence Route Selection 626

OSPF Load Balancing 627

Injecting Default Routes 627

OSPFv3 Verification and Troubleshooting 628

OSPFv3 Interfaces 630

Verifying OSPFv3 Interfaces 630

Troubleshooting OSPFv3 Interfaces 631

OSPFv3 Neighbors 632

Verifying OSPFv3 Neighbors 632

Troubleshooting OSPFv3 Neighbors 633

OSPFv3 LSDB and LSAs 636

The Issue of IPv6 MTU 636

OSPFv3 Metrics and IPv6 Routes 638

Verifying OSPFv3 Interface Cost and Metrics 638

Troubleshooting IPv6 Routes Added by OSPFv3 640

Chapter Review 642

Chapter 24 Implementing EIGRP for IPv6 644

"Do I Know This Already?" Quiz 644

Foundation Topics 646

EIGRP for IPv6 Configuration 646

EIGRP for IPv6 Configuration Basics 647

EIGRP for IPv6 Configuration Example 648

Other EIGRP for IPv6 Configuration Settings 650

Setting Bandwidth and Delay to Influence EIGRP for IPv6 Route Selection 650

EIGRP Load Balancing 651

EIGRP Timers 652

EIGRP for IPv6 Verification and Troubleshooting 653

EIGRP for IPv6 Interfaces 654

EIGRP for IPv6 Neighbors 656

EIGRP for IPv6 Topology Database 657

EIGRP for IPv6 Routes 659

Chapter Review 661

Chapter 25 IPv6 Access Control Lists 664

"Do I Know This Already?" Quiz 664

Foundation Topics 666

IPv6 Access Control List Basics 666

Similarities and Differences Between IPv4 and IPv6 ACLs 666

ACL Location and Direction 667

IPv6 Filtering Policies 668

ICMPv6 Filtering Caution 668

Capabilities of IPv6 ACLs 669

Limitations of IPv6 ACLs 669

Matching Tunneled Traffic 670

IPv4 Wildcard Mask and IPv6 Prefix Length 670

ACL Logging Impact 670

Router Originated Packets 670

Configuring Standard IPv6 ACLs 671

Configuring Extended IPv6 ACLs 674

Examples of Extended IPv6 ACLs 676

Practice Building ipv6 access-list Commands 678

Other IPv6 ACL Topics 679

Implicit IPv6 ACL Rules 679

An Example of Filtering ICMPv6 NDP and the Negative Effects 679

How to Avoid Filtering ICMPv6 NDP Messages 683

IPv6 ACL Implicit Filtering Summary 684

IPv6 Management Control ACLs 685

Chapter Review 686

Part VI Review 688

Part VII Miscellaneous 691

Chapter 26 Network Management 692

"Do I Know This Already?" Quiz 692

Foundation Topics 694

Simple Network Management Protocol 694

SNMP Concepts 695

SNMP Variable Reading and Writing: SNMP Get and Set 696

SNMP Notifications: Traps and Informs 696

The Management Information Base 697

Securing SNMP 698

Implementing SNMP Version 2c 699

Configuring SNMPv2c Support for Get and Set 699

Configuring SNMPv2c Support for Trap and Inform 701

Verifying SNMPv2c Operation 702

Implementing SNMP Version 3 704

SNMPv3 Groups 705

SNMPv3 Users, Passwords, and Encryption Keys 707

Verifying SNMPv3 708

Implementing SNMPv3 Notifications (Traps and Informs) 710

Summarizing SNMPv3 Configuration 711

IP Service Level Agreement 712

An Overview of IP SLA 713

Basic IP SLA ICMP-Echo Configuration 714

Troubleshooting Using IP SLA Counters 715

Troubleshooting Using IP SLA History 716

SPAN 718

SPAN Concepts 718

The Need for SPAN When Using a Network Analyzer 719

SPAN Session Concepts 720

Configuring Local SPAN 721
SPAN Session Parameters for Troubleshooting 724
Choosing to Limit SPAN Sources 725
Chapter Review 726
Chapter 27 Cloud Computing 730
"Do I Know This Already?" Quiz 730
Foundation Topics 732
Cloud Computing Concepts 732
Server Virtualization 732
Cisco Server Hardware 732
Server Virtualization Basics 733
Networking with Virtual Switches on a Virtualized Host 735
The Physical Data Center Network 736
Workflow with a Virtualized Data Center 737
Cloud Computing Services 739
Private Cloud 739
Public Cloud 741
Cloud and the "As a Service" Model 741
Infrastructure as a Service 742
Software as a Service 743
(Development) Platform as a Service 743
WAN Traffic Paths to Reach Cloud Services 744
Enterprise WAN Connections to Public Cloud 744
Accessing Public Cloud Services Using the Internet 745
Pros and Cons with Connecting to Public Cloud with Internet 745
Private WAN and Internet VPN Access to Public Cloud 746
Pros and Cons with Connecting to Cloud with Private WANs 747
Intercloud Exchanges 748
Summarizing the Pros and Cons of Public Cloud WAN Options 749
A Scenario: Branch Offices and the Public Cloud 749
Migrating Traffic Flows When Migrating to Email SaaS 750
Branch Offices with Internet and Private WAN 751
Virtual Network Functions and Services 752
Virtual Network Functions: Firewalls and Routers 752
DNS Services 754
Address Assignment Services and DHCP 756
NTP 757
Chapter Review 758

Chapter 28 SDN and Network Programmability 760

"Do I Know This Already?" Quiz 761

Foundation Topics 762

SDN and Network Programmability Basics 762

The Data, Control, and Management Planes 762

The Data Plane 762

The Control Plane 763

The Management Plane 764

Cisco Switch Data Plane Internals 765

Controllers and Network Architecture 766

Controllers and Centralized Control 766

The Southbound Interface 767

The Northbound Interface 768

SDN Architecture Summary 770

Examples of Network Programmability and SDN 770

Open SDN and OpenFlow 771

The OpenDaylight Controller 771

Cisco Open SDN Controller 772

The Cisco Application Centric Infrastructure 773

The Cisco APIC Enterprise Module 774

Comparing the Three Examples 776

Cisco APIC-EM Path Trace ACL Analysis Application 777

APIC-EM Path Trace App 777

APIC-EM Path Trace ACL Analysis Tool Timing and Exam Topic 778

Chapter Review 778

Part VII Review 780

Part VIII Final Prep 783

Chapter 29 Final Review 784

Advice About the Exam Event 784

Learn the Question Types Using the Cisco Certification Exam Tutorial 784

Think About Your Time Budget Versus Number of Questions 785

A Suggested Time-Check Method 786

Miscellaneous Pre-Exam Suggestions 786

Exam-Day Advice 787

Reserve the Hour After the Exam in Case You Fail 788

Exam Review 788

Take Practice Exams 789

Practicing Taking the ICND2 or CCNA R&S Exam 790

Advice on How to Answer Exam Questions 790

Taking Other Practice Exams 792

Find Knowledge Gaps Through Question Review 792

Practice Hands-On CLI Skills 794

Review Mind Maps from Part Review 795

Do Labs 795

Assess Whether You Are Ready to Pass (and the Fallacy of Exam Scores) 796

Study Suggestions After Failing to Pass 797

Other Study Tasks 798

Final Thoughts 799

Part IX Appendixes 801

Appendix A Numeric Reference Tables 803

Appendix B CCNA ICND2 200-105 Exam Updates 810

Glossary 813

Index 852

DVD Appendixes

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

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

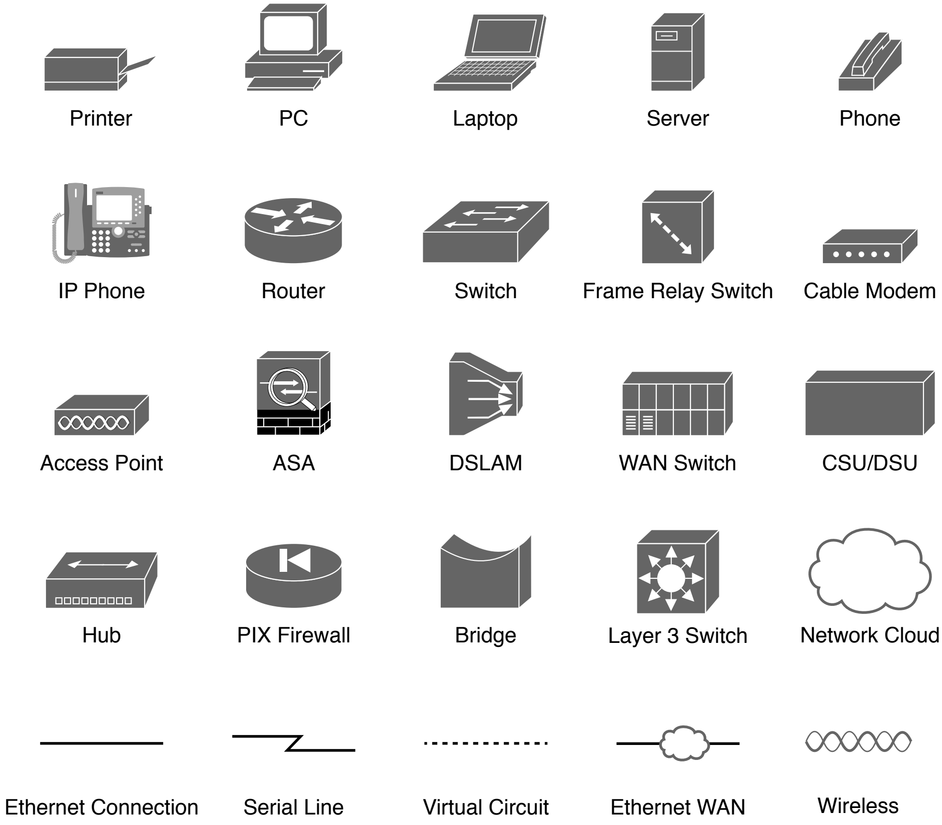
Appendix L Exam Topic Cross Reference

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 9781587205798 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.

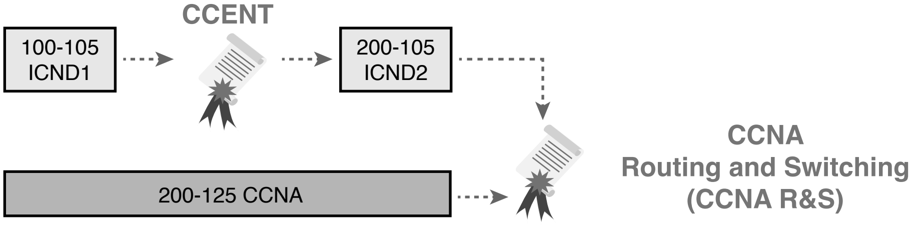


Figure I-1 *Cisco Entry-Level Certifications and Exams*

Note that Cisco has begun referencing some exams with a version number on some of their websites. 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:

- **"Do I Know This Already?" quiz:** Each chapter begins with a prechapter quiz.
- **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.

Figure I-2 shows how each chapter uses these three key elements. You start with the "Do I Know This Already?" (DIKTA) quiz. You can use the score to determine whether you already know a lot, or not so much, and determine how to approach reading the Foundation Topics (that is, the technology content in the chapter). When finished with the Foundation Topics, use the Chapter Review tasks to start working on mastering your memory of the facts and skills with configuration, verification, and troubleshooting.

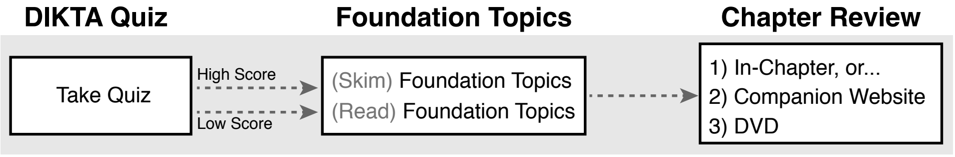


Figure I-2 *Three Primary Tasks for a First Pass Through Each Chapter*

In addition to these three 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.

- **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.
- **Review DIKTA Questions:** Re-answering the DIKTA questions from the chapter is a useful way to review facts. The Part Review element that comes at the end of each book Part suggests that you repeat the DIKTA questions. The Part Review also suggests using the Pearson IT Certification Practice Test (PCPT) exam software that comes with the book, for extra practice in answering multiple-choice questions on a computer.

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-3 lists the titles of the parts and identifies the chapters in those parts by chapter numbers.

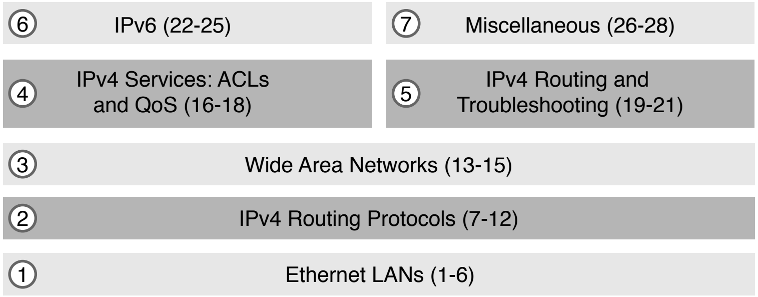

6
IPv6 (22-25)
7
Miscellaneous (26-28)
4
IPv4 Services: ACLs and QoS (16-18)
5
IPv4 Routing and Troubleshooting (19-21)
3
Wide Area Networks (13-15)
2
IPv4 Routing Protocols (7-12)
1
Ethernet LANs (1-6)

Figure I-3 *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 DIKTA 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:

- **DVD-based practice exams:** The companion DVD contains the powerful Pearson IT Certification Practice Test (PCPT) exam engine. You can take simulated ICND2 exams, as well as CCNA exams, with the DVD and activation code included in this book. (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:** If you are interested in obtaining an eBook version of this title, we have included a special offer on a coupon card inserted in the DVD sleeve in the back of the book. This offer allows you to purchase the *CCNA Routing and Switching ICND2 200-105 Official Cert Guide Premium Edition eBook and Practice Test* at a 70 percent discount off the list price. In addition to three versions of the eBook, PDF (for reading on your computer), EPUB (for reading on your tablet, mobile device, or Nook or other eReader), and Mobi (the native Kindle version), you also receive additional practice test questions and enhanced practice test features.
- **Mentoring Videos:** The DVD included with this book includes four other instructional videos about the following topics: OSPF, EIGRP, EIGRP metrics, plus PPP and CHAP.
- **Companion website:** The website http://www.ciscopress.com/title/9781587205798 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
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 registering your book on the Cisco Press website. To do so, simply go to http://www.ciscopress.com/register and enter the ISBN of the print book: 9781587205798. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book's companion website.

If you buy the *CCNA Routing and Switching ICND2 200-105 Official Cert Guide Premium Edition eBook and Practice Test* from Cisco Press, 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.

If you buy the eBook from some other bookseller, the very last page of your eBook file will contain instructions for how to register the book and access the companion website. The steps are the same as noted earlier for those who buy the print book but do not have a DVD drive.

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 'Do I Know This Already?' 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 100-101 book).
- Chapter 16, "Basic IPv4 Access Control Lists" (Chapter 25 in the ICND1 100-101 book).

- Chapter 17, "Advanced IPv4 Access Control Lists" (Chapter 26 in the ICND1 100-101 book).
- Chapter 21, "Troubleshooting IPv4 Routing" (Chapter 24 in the ICND1 100-101 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 100-101 book, you can move more quickly through the above four chapters in this book. If you did not read the ICND1 100-101 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 DIKTA chapter quizzes using PCPT.

NOTE The right to use the exams associated with this book is based on an activation code. For those with a paper book, the code is in the DVD sleeve at the back of the book. (Flip over the paper with the exam activation code to find a one-time-use coupon code for 70 percent off the purchase of the *CCNA Routing and Switching ICND2 200-105 Official Cert Guide, Premium Edition eBook and Practice Test*.) For those who purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the activation code will be populated on your account page after purchase. For those who purchase a Kindle edition, the access code will be supplied directly from Amazon. Note that if you purchase an eBook version from any other source, the practice test is not included, as other vendors are not able to vend the required unique access code. *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-4.

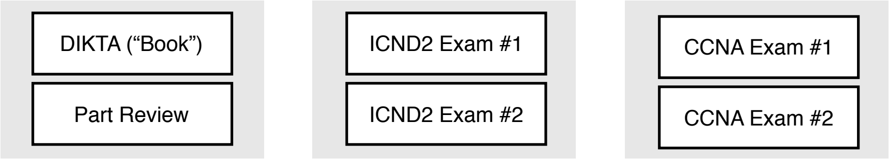


Figure I-4 *PCPT Exams/Exam Databases and When to Use Them*

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-4 begins to suggest a plan, spelled out here:

- During Part Review, use PCPT to review the DIKTA questions for that part, using study mode.
- During Part Review, use the questions built specifically for Part Review (the Part Review questions) for that part of the book, using study mode.
- Save the remaining exams to use with 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 Only DIKTA Questions by Chapter or Part

Most chapters begin with a DIKTA quiz. You can take the quiz to start a chapter, take it again during Chapter Review for more practice, and, as suggested in the "Part Review" sections, repeat the questions for all chapters in the same part.

You can use the DIKTA quiz as printed in the book, or use the PCPT software. The book lists the questions, with the letter answers on the page following the quiz. Appendix C, on the DVD, lists the answers along with an explanation; you might want to keep that PDF handy.

Using PCPT for these questions has some advantages. It gives you a little more practice in how to read questions from testing software. Also, the explanations to the questions are conveniently located in the PCPT software.

To view these DIKTA questions inside the PCPT software, you need to select **Book Questions**, which is the way PCPT references questions found inside the printed book. Then you have to deselect all chapters (with a single click), and then select one or more chapters, as follows:

Step 1. Start the PCPT software.

Step 2. From the main (home) menu, select the item for this product, with a name like *CCNA Routing and Switching ICND2 200-105 Official Cert Guide*, and click **Open Exam**.

Step 3. The top of the next window that appears should list some exams; check the **ICND2 Book Questions** box, and uncheck the other boxes. This selects the "book" questions (that is, the DIKTA questions from the beginning of each chapter).

Step 4. On this same window, click at the bottom of the screen to deselect all objectives (chapters). Then select the box beside each chapter in the part of the book you are reviewing.

Step 5. Select any other options on the right side of the window.

Step 6. Click **Start** to start reviewing the questions.

How to View Part Review Questions

The exam databases you get with this book include a database of questions created solely for study during the Part Review process. DIKTA questions focus more on facts, 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 DIKTA/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-5 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.

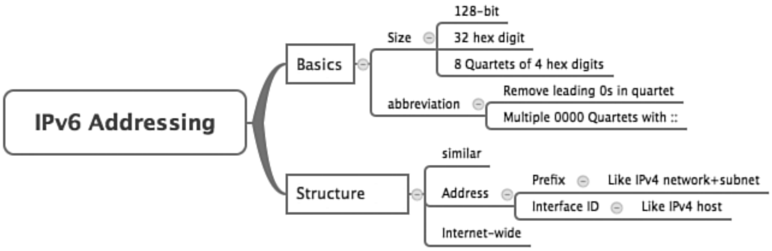


Figure I-5 *Sample Mind Map*

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-6 *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.

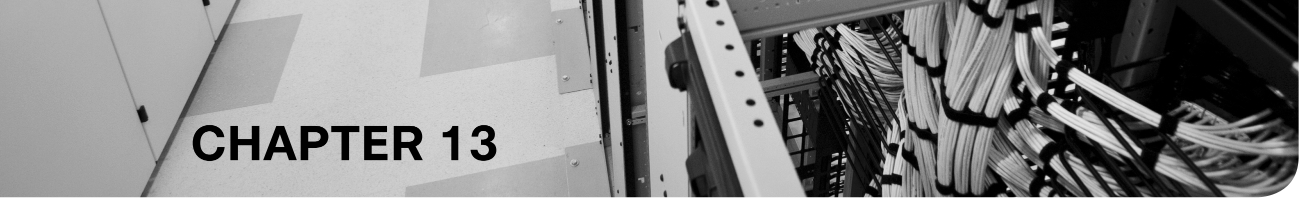
This book does not tell you what option to use, but you should plan on getting some hands-on practice somehow. The important thing to know is that most people need to practice using the Cisco CLI to be ready to pass these exams.

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.



CHAPTER 13

Implementing Point-to-Point WANs

This chapter covers the following exam topics:

3.0 WAN Technologies

3.1 Configure and verify PPP and MLPPP on WAN interfaces using local authentication

Leased-line WANs—also known as serial links—require much less thought than many other topics, at least to the depth required for the CCENT and CCNA R&S exams. That simplicity allows the Cisco exams to discuss leased lines briefly for the ICND1 exam, while using leased lines as part of larger discussions of IP routing.

This chapter finally takes the discussion of leased-line WANs deeper than has been discussed so far. This chapter briefly repeats the leased line concepts from the ICND1 book, to lay a foundation to discuss other concepts. More important, this chapter looks at the configuration, verification, and troubleshooting steps for leased lines that use the familiar High-level Data Link Control (HDLC) data-link protocol and the Point-to-Point Protocol (PPP).

This chapter breaks the material down into three major sections. The first looks at leased-line WANS that use HDLC, by reviewing and adding details about the physical links themselves, along with HDLC (and related) configuration. The second major section discusses PPP, an alternate data-link protocol that you can use instead of HDLC, with a focus on concepts and configuration. The final major section then discusses typical root causes of serial link problems and how to find those problems.

"Do I Know This Already?" Quiz

Take the quiz (either here, or use the PCPT software) if you want to use the score to help you decide how much time to spend on this chapter. The answers are at the bottom of the page following the quiz, and the explanations are in DVD Appendix C and in the PCPT software.

Table 13-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Leased-Line WANs with HDLC	1–2
Leased-Line WANs with PPP	3–6
Troubleshooting Serial Links	7

1. In the cabling for a leased line, which of the following usually connects to a four-wire line provided by a telco?

a. Router serial interface without internal CSU/DSU

b. CSU/DSU

c. Router serial interface with internal transceiver

d. Switch serial interface

2. Two routers connect with a serial link, each using its S0/0/0 interface. The link is currently working using PPP. The network engineer wants to migrate to use the Cisco-proprietary HDLC that includes a protocol type field. Which of the following commands can be used to migrate to HDLC successfully? (Choose two answers.)

   a. **encapsulation hdlc**

   b. **encapsulation cisco-hdlc**

   c. **no encapsulation ppp**

   d. **encapsulation-type auto**

3. Which of the following PPP authentication protocols authenticates a device on the other end of a link without sending any password information in clear text?

   a. MD5

   b. PAP

   c. CHAP

   d. DES

4. Two routers have no initial configuration whatsoever. They are connected in a lab using a DTE cable connected to R1 and a DCE cable connected to R2, with the DTE and DCE cables then connected to each other. The engineer wants to create a working PPP link by configuring both routers. Which of the following commands are required in the R1 configuration for the link to reach a state in which R1 can ping R2's serial IP address, assuming that the physical back-to-back link physically works? (Choose two answers.)

   a. **encapsulation ppp**

   b. **no encapsulation hdlc**

   c. **clock rate**

   d. **ip address**

5. Consider the following excerpt from the output of a **show** command:

```
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

   Which of the following are true about this router's S0/0/1 interface? (Choose two answers.)

   a. The interface is using HDLC.

   b. The interface is using PPP.

   c. The interface currently cannot pass IPv4 traffic.

   d. The link should be able to pass PPP frames at the present time.

6. Two routers, R1 and R2, connect to each other using three serial links. The network engineer configures these links to be part of the same multilink PPP group, along with configuring CHAP configuration, IPv4, and OSPFv2 using interface configuration. Which of the following answers list a configuration command along with the correct configuration mode for that command? (Choose two answers.)
   a. **encapsulation ppp** while in multilink interface configuration mode
   b. **ip address** address mask while in serial interface configuration mode
   c. **ppp authentication chap** while in multilink interface configuration mode
   d. **ip ospf 1 area 0** while in serial interface configuration mode
   e. **ppp multilink** while in serial interface configuration mode

7. Consider the following excerpt from the output of a **show interfaces** command on an interface configured to use PPP:

```
Serial0/0/1 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.168.2.1/24
```

   A ping of the IP address on the other end of the link fails. Which of the following are reasons for the failure, assuming that the problem listed in the answer is the only problem with the link? (Choose two answers.)
   a. The CSU/DSU connected to the other router is not powered on.
   b. The IP address on the router at the other end of the link is not in subnet 192.168.2.0/24.
   c. CHAP authentication failed.
   d. The router on the other end of the link has been configured to use HDLC.
   e. None of the above.

Foundation Topics

Leased-Line WANs with HDLC

A physical leased-line WAN works a lot like in an Ethernet crossover cable connecting two routers, but with no distance limitations. As shown in Figure 13-1, each router can send at any time (full duplex). The speed is also symmetric, meaning that both routers send bits at the same speed.

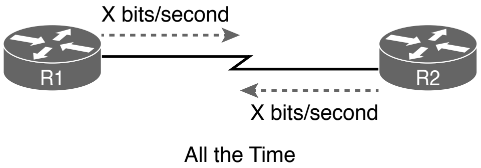


Figure 13-1 *Leased Line: Same Speed, Both Directions, Always On*

Although the leased line provides a physical layer bit transmission facility, routers also need to use a data link protocol on the WAN link to send bits over the link. The story should be familiar by now: routers receive frames in LAN interfaces, and then the router de-encapsulates the network layer packet. Before forwarding the packet, the router encapsulates the packet inside a WAN data link protocol like High-level Data Link Control (HDLC), as shown at Step 2 of Figure 13-2.

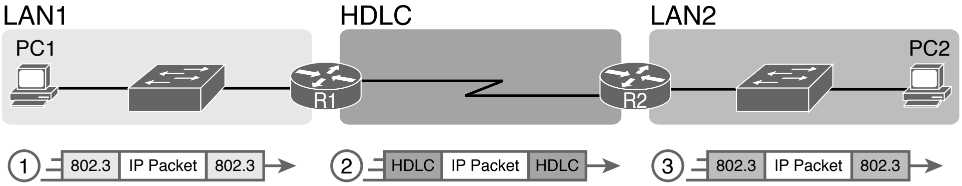


Figure 13-2 *Routers and Their Use of HDLC to Encapsulate Packets*

These first two figures review some of the Layer 1 and Layer 2 details, respectively, of leased-line WANs. This first major section of this chapter begins by discussing these links again, first with the Layer 1 details, followed by the Layer 2 details. This section ends with an explanation of HDLC configuration details.

Layer 1 Leased Lines

Leased lines have been around a long time, roughly 20 years longer than LANs. However, they still exist today as a WAN service.

As a result of their long history in the market, the networking world has used a large number of different terms. First, the term *leased line* refers to the fact that the company using the leased line does not own the line, but instead pays a monthly lease fee to use it. Often, you lease the service from a telephone company, or *telco*. However, many people today use the generic term *service provider* to refer to a company that provides any form of WAN connectivity, including Internet services. Table 13-2 lists some of those names so that you can understand the different terms you will encounter in a real networking job.

Table 13-2 Different Names for a Leased Line

Name	Meaning or Reference
Leased circuit, circuit	The words *line* and *circuit* are often used as synonyms in telco terminology; *circuit* makes reference to the electrical circuit between the two endpoints.
Serial link, serial line	The words *link* and *line* are also often used as synonyms. *Serial* in this case refers to the fact that the bits flow serially and that routers use serial interfaces.
Point-to-point link, point-to-point line	Refers to the fact that the topology stretches between two points, and two points only. (Some older leased lines allowed more than two devices.)
T1	A specific type of leased line that transmits data at 1.544 megabits per second (1.544 Mbps).
WAN link, link	Both these terms are very general, with no reference to any specific technology.

Answers to the "Do I Know This Already?" quiz:

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

The Physical Components of a Leased Line

To create a leased line, the telco must create some physical transmission path between the two routers on the ends of the link. The physical cabling must leave the buildings where each router sits. Then the telco must create the equivalent of a two-pair circuit from end to end, with one circuit to send data in each direction (full duplex). Figure 13-3 shows one such example, in which the telco uses a couple of traditional central office (CO) switches to create a short leased line between two routers.

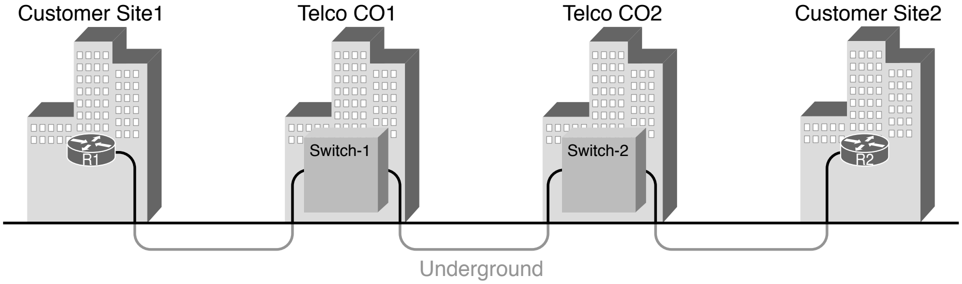


Figure 13-3 *Possible Cabling Inside a Telco for a Short Leased Line*

The details in the center of Figure 13-3 probably show more than you ever need to know about leased-line WANs, at least from the enterprise customer perspective. More commonly, most network engineers think more about a leased line from the perspective of Figure 13-4, which shows a few key components and terms for the equipment on the ends of a leased line, as follows:

Customer premises equipment (CPE): This telco term refers to the gear that sits at their customers' sites on the ends on the link.

Channel service unit/data service unit (CSU/DSU): This device provides a function called *clocking*, in which it physically controls the speed and timing at which the router serial interface sends and receives each bit over the serial cable.

Serial cable: This is a short cable that connects the CSU and the router serial interface.

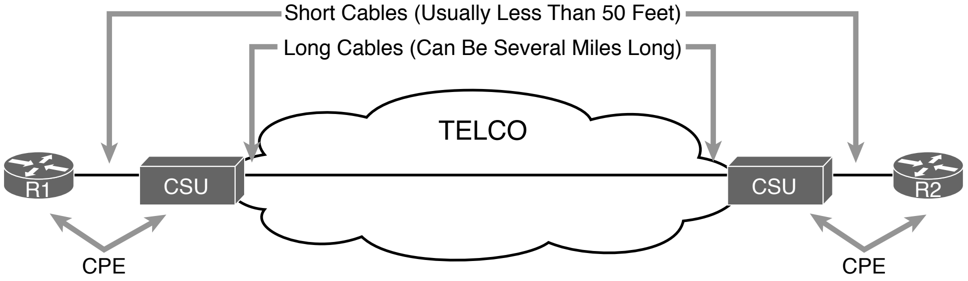

Short Cables (Usually Less Than 50 Feet)
Long Cables (Can Be Several Miles Long)
TELCO
R1
CSU
CSU
R2
CPE
CPE

Figure 13-4 *Point-to-Point Leased Line: Components and Terminology*

The CPE includes several separately orderable parts. When using an external CSU/DSU, a serial cable must be used to connect the CSU to the router serial interface. These serial interfaces usually exist as part of a removable card on the router, called either WAN interface cards (WIC), High-speed WICs (HWIC), or Network Interface Modules (NIM). Most of the serial interfaces use one style (size/shape) of physical connector called a smart serial connector, whereas the CSU has one of several other types of connectors. So, when installing the leased line, the engineer must choose the correct cable type, with connectors to match the WIC on one end and the CSU/DSU on the other. Figure 13-5 shows a drawing of one type of serial cable, with the smart serial connector on the left, and the popular V.35 connector on the right. The figure shows a side view of the entire cable, plus direct views into the connector on the ends of the cable.

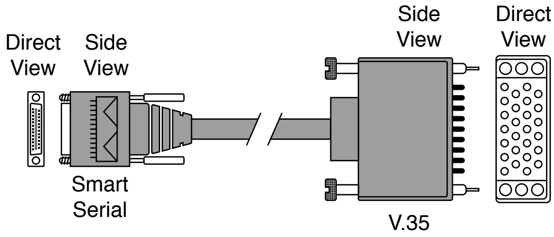


Figure 13-5 *Serial Cables Used Between a CSU and a Router*

Today, many leased lines make use of Cisco WICs with an integrated CSU/DSU. That is, the WIC hardware includes the same functions as a CSU/DSU, so an external CSU/DSU is not needed. Compared to Figure 13-4, the external CSU/DSU and serial cable on each end are not needed, with the cable from the telco connecting directly to the WIC.

Figure 13-6 shows a photo of a router with two NIM slots. Each slot currently shows a faceplate with no NIM cards installed. The foreground of the figure shows a NIM with two serial ports, with smart serial interfaces. The cable end on the left of the drawing in Figure 13-5 would attach to one of these smart serial ports on the NIM in Figure 13-6.

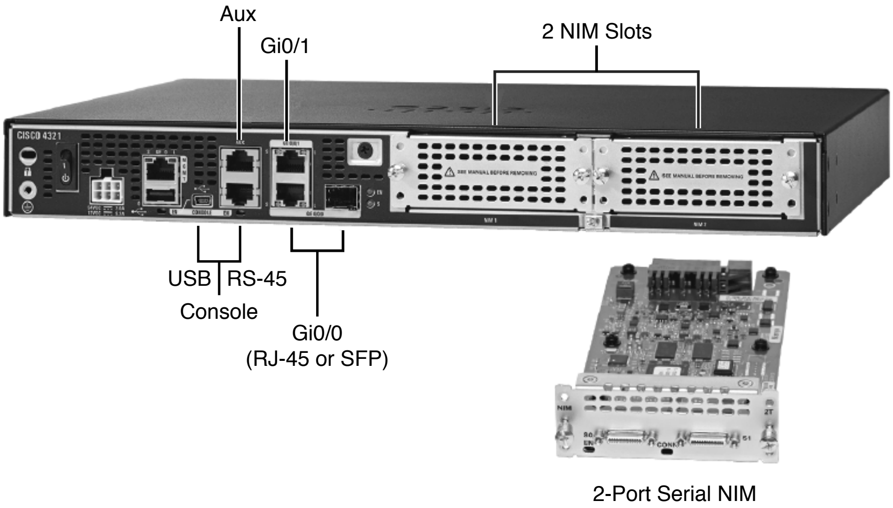


Figure 13-6 *Photo of Router with Serial NIM on the Right*

Telcos offer a wide variety of speeds for leased lines. However, a telco customer cannot pick just any speed. Instead, the speeds follow the standards of an age-old technology called the T-carrier system.

Back in the 1950s and 1960s, the U.S.-based Bell companies developed and deployed digital voice and the T-carrier system. As part of that work, they standardized different transmission speeds, including 64 Kbps, 1.544 Mbps, and 44.736 Mbps.

Those same Bell companies developed time-division multiplexing (TDM) technology that let them combine multiples of these base speeds onto a single line. For instance, one popular standard, a Digital Signal level 1 (DS1), or T1, combines 24 DS0s (at 64 Kbps) plus 8 Kbps of overhead into one physical line that runs at 1.544 Mbps. However, to allow flexibility of speeds offered to customers, the telco could install a T1 line to many sites, but run some at slower speeds and some at faster speeds—as long as those speeds were multiples of 64 Kbps.

Now back to the idea of the speed of a leased line. What can you actually buy? Basically, at slower speeds, you get any multiple of 64 Kbps, up to T1 speed. At faster speeds, you can get multiples of T1 speed, up to T3 speed. Table 13-3 summarizes the speeds typically seen in the United States, with a few from Europe.

Key Topic

Table 13-3 WAN Speed Summary

Names of Line	Bit Rate
DS0	64 Kbps
Fractional T1	Multiples of 64 Kbps, up to 24X
DS1 (T1)	1.544 Mbps (24 DS0s, for 1.536 Mbps, plus 8 Kbps overhead)
E1 (Europe)	2.048 Mbps (32 DS0s)
Fractional T3	Multiples of 1.536 Mbps, up to 28X
DS3 (T3)	44.736 Mbps (28 DS1s, plus management overhead)
E3 (Europe)	Approx. 34 Mbps (16 E1s, plus management overhead)

The Role of the CSU/DSU

For our last bit of discussion about WAN links in a working enterprise internetwork, next consider the role of the CSU/DSU (called CSU for short). For the sake of discussion, the next few paragraphs, leading up to Figure 13-7, assume a leased line with external CSU/DSUs, like earlier in Figure 13-4.

The CSU sits between the telco leased line and the router; it understands both worlds and their conventions at Layer 1. On the telco side, that means the CSU connects to the line from the telco, so it must understand all these details about the T-carrier system, TDM, and the speed used by the telco. On the router side of the equation, the CSU connects to the router, with roles called the DCE and DTE, respectively. The CSU, acting as DCE (data circuit-terminating equipment), controls the speed of the router serial interface. The router, acting as DTE (data terminal equipment), is controlled by the clocking signals from the CSU (DCE). That is, the CSU tells the router when to send and receive bits; the router attempts to send and receive bits only when the DCE creates the correct electrical impulses (called clocking) on the cable. Figure 13-7 shows a diagram of those main concepts of the role of the CSU/DSU.

Key Topic

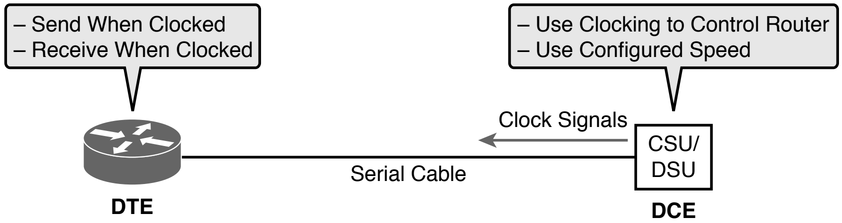


Figure 13-7 *DCE and DTE Roles for a CSU/DSU and a Router Serial Interface*

Building a WAN Link in a Lab

On a practical note, to prepare for the CCENT and CCNA R&S exams, you might choose to buy some used router and switch hardware for hands-on practice. If you do, you can create the equivalent of a leased line, without a real leased line from a telco, and without CSU/DSUs, just using a cabling trick. This short discussion tells you enough information to create a WAN link in your home lab.

First, when building a real WAN link with a real telco facility between sites, the serial cables normally used between a router and an external CSU/DSU are called *DTE cables*. That is, the serial cables in earlier Figure 13-4 are DTE cables.

You can create an equivalent WAN link just by connecting two routers' serial interfaces using one DTE cable and a slightly different DCE cable, with no CSUs and with no leased line from the telco. The DCE cable has a female connector, and the DTE cable has a male connector, which allows the two cables to be attached directly. That completes the physical connection, providing a path for the data. The DCE cable also does the equivalent of an Ethernet crossover cable by swapping the transmit and receive wire pairs, as shown in Figure 13-8.

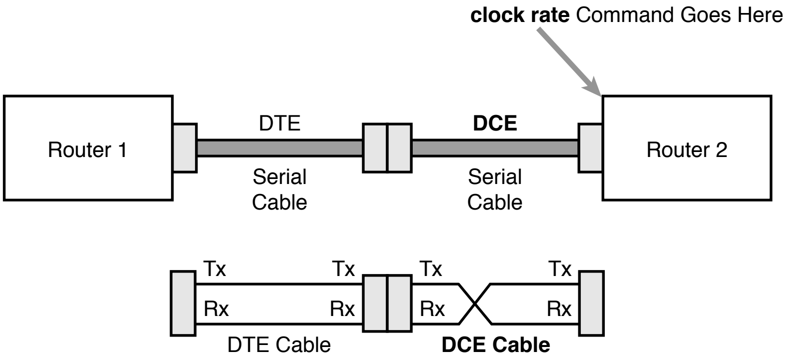


Figure 13-8 *Serial Cabling Uses a DTE Cable and a DCE Cable*

The figure shows the cable details at the top, with the wiring details at the bottom. In particular, at the bottom of the figure, note that the DTE serial cable acts as a straight-through cable and does not swap the transmit and receive pair, whereas the DCE cable does swap the pairs.

NOTE Many vendors, for convenience, sell a single cable that combines the two cables shown in Figure 13-8 into a single cable. Search online for "Cisco serial crossover" to find examples.

Finally, to make the link work, the router with the DCE cable installed must provide clocking. A router serial interface can provide clocking, but it can do so only if a DCE cable is connected to the interface and by the configuration of the **clock rate** command. Newer IOS versions will sense the presence of a DCE cable and automatically set a clock rate, so that the link will work, but old IOS versions require that you configure the **clock rate** command.

Layer 2 Leased Lines with HDLC

A leased line provides a Layer 1 service. It promises to deliver bits between the devices connected to the leased line. However, the leased line itself does not define a data link layer protocol to be used on the leased line. HDLC provides one option for a data link protocol for a leased line.

HDLC has only a few big functions to perform with the simple point-to-point topology of a point-to-point leased line. First, the frame header lets the receiving router know that a new frame is coming. Plus, like all the other data link protocols, the HDLC trailer has a Frame Check Sequence (FCS) field that the receiving router can use to decide whether the frame had errors in transit, and if so, discard the frame.

Cisco adds another function to the ISO standard HDLC protocol by adding an extra field (a Type field) to the HDLC header, creating a Cisco-specific version of HDLC, as shown in Figure 13-9. The Type field allows Cisco routers to support multiple types of network layer packets to cross the HDLC link. For example, an HDLC link between two Cisco routers can forward both IPv4 and IPv6 packets because the Type field can identify which type of packet is encapsulated inside each HDLC frame.

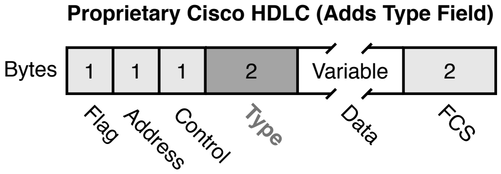


Figure 13-9 *Cisco HDLC Framing*

Today, the HDLC Address and Control fields have little work to do. For instance, with only two routers on a link, when a router sends a frame, it is clear that the frame is sent to the only other router on the link. Both the Address and Control fields had important purposes in years past, but today they are unimportant.

Routers use HDLC just like any other data link protocol used by routers: to move packets to the next router. Figure 13-10 shows three familiar routing steps, with the role of HDLC sitting at Step 2.

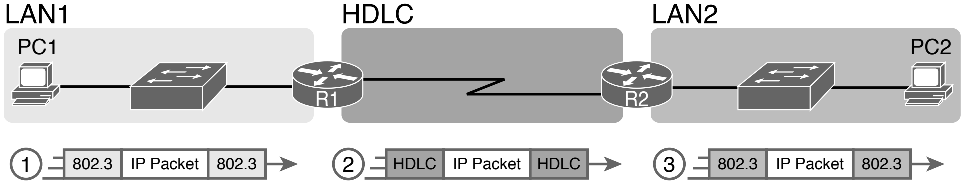


Figure 13-10 *General Concept of Routers De-encapsulating and Re-encapsulating IP Packets*

Here is a walkthrough of the steps in the figure:

1. To send the IP packet to router R1, PC1 encapsulates the IP packet in an Ethernet frame.
2. Router R1 de-encapsulates (removes) the IP packet, encapsulates the packet into an HDLC frame using an HDLC header and trailer, and forwards the HDLC frame to router R2.
3. Router R2 de-encapsulates (removes) the IP packet, encapsulates the packet into an Ethernet frame, and forwards the Ethernet frame to PC2.

In summary, a leased line with HDLC creates a WAN link between two routers so that they can forward packets for the devices on the attached LANs. The leased line itself provides the physical means to transmit the bits, in both directions. The HDLC frames provide the means to encapsulate the network layer packet correctly so it crosses the link between routers.

Configuring HDLC

Think back to router Ethernet interfaces for a moment. Router Ethernet interfaces require no configuration related to Layers 1 and 2 for the interface to be up and working, forwarding IP traffic. The Layer 1 details occur by default once the cabling has been installed correctly. Router Ethernet interfaces, of course, use Ethernet as the data link protocol by default. The router only needs to configure an IP address on the interface, and possibly enable the interface with the **no shutdown** command if the interface is in an "administratively down" state.

Similarly, serial interfaces on Cisco routers need no specific Layer 1 or 2 configuration commands. For Layer 1, the cabling needs to be completed, of course, but the router attempts to use the serial interface once the **no shutdown** command is configured. For Layer 2, IOS defaults to use HDLC on serial interfaces. As on Ethernet interfaces, router serial interfaces usually only need an **ip address** command, and possibly the **no shutdown** command, assuming both routers' interfaces otherwise have default settings.

Config Checklist

However, many optional commands exist for serial links. The following list outlines some configuration steps, listing the conditions for which some commands are needed, plus commands that are purely optional:

Step 1. Use the **ip address** *address mask* command in interface configuration mode to configure the interface IP address.

Step 2. The following tasks are required only when the specifically listed conditions are true:

A. If an **encapsulation** *protocol* interface subcommand already exists, for a non-HDLC protocol, use the **encapsulation hdlc** command in interface configuration mode to enable HDLC. Alternatively, use the **no encapsulation** *protocol* command in interface configuration mode to use the default setting of HDLC as the data link protocol.

B. If the interface line status is administratively down, use the **no shutdown** command in interface configuration mode to enable the interface.

- **C.** If the serial link is a back-to-back serial link in a lab (or a simulator), use the **clock rate** *speed* command in interface configuration mode to configure the clocking rate. Use this command only on the one router with the DCE cable (per the **show controllers serial** *number* command).

Step 3. The following steps are always optional and have no impact on whether the link works and passes IP traffic:

- **A.** Use the **bandwidth** *speed-in-kbps* command in interface configuration mode to configure the link's documented speed so that it matches the actual clock rate of the link.
- **B.** For documentation purposes, use the **description** *text* command in interface configuration mode to configure a description of the purpose of the interface.

In practice, when you configure a Cisco router with no preexisting interface configuration and install a normal production serial link with CSU/DSUs, the **ip address** and **no shutdown** commands are likely the only configuration commands you would need.

Figure 13-11 shows a sample internetwork, and Example 13-1 shows the matching HDLC configuration. In this case, the serial link was created with a back-to-back serial link in a lab, requiring Steps 1 (**ip address**) and 2C (**clock rate**) from the preceding list. It also shows optional Step 3B (**description**).

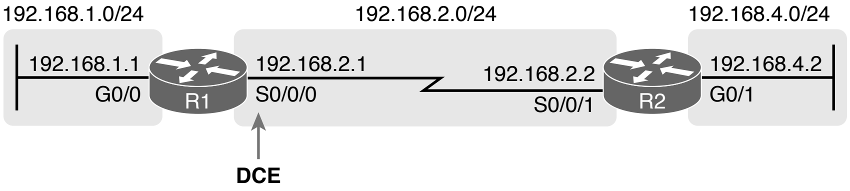


Figure 13-11 *Typical Serial Link Between Two Routers*

Example 13-1 *HDLC Configuration*

```
R1# show running-config
! Note - only the related lines are shown
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 192.168.2.1 255.255.255.0
 description link to R2
 clock rate 2000000
!
router eigrp 1
 network 192.168.1.0
 network 192.168.2.0
```

The configuration on R1 is relatively simple. The matching configuration on R2's S0/0/1 interface simply needs an **ip address** command plus the default settings of **encapsulation hdlc** and **no shutdown**. The **clock rate** command would not be needed on R2 because R1 has the DCE cable, so R2 must be connected to a DTE cable.

Example 13-2 lists two commands that confirm the configuration on R1 and some other default settings. First, it lists the output from the **show controllers** command for S0/0/0, which confirms that R1 indeed has a DCE cable installed and that the clock rate has been set to 2000000 bps. The **show interfaces S0/0/0** command lists the various configuration settings near the top, including the default encapsulation value (HDLC) and default bandwidth setting on a serial interface (1544, meaning 1544 Kbps or 1.544 Mbps). It also lists the IP address, prefix-style mask (/24), and description, as configured in Example 13-1.

Example 13-2 *Verifying the Configuration Settings on R1*

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is SCC
DCE V.35, clock rate 2000000
! lines omitted for brevity

R1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     276 packets input, 19885 bytes, 0 no buffer
     Received 96 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     284 packets output, 19290 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     7 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Finally, the router uses the serial interface only if it reaches an up/up interface status, as shown in the first line of the output of the **show interfaces S0/0/0** command in Example 13-2. Generally speaking, the first status word refers to Layer 1 status, and the second refers to Layer 2 status. For a quicker look at the interface status, instead use either the **show ip interface brief** or **show interfaces description** commands, as listed in Example 13-3.

Example 13-3 *Brief Lists of Interfaces and Interface Status*

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.1.1     YES manual up                    up
GigabitEthernet0/1         unassigned      YES manual administratively down down
Serial0/0/0                192.168.2.1     YES manual up                    up
Serial0/0/1                unassigned      YES NVRAM  administratively down down
Serial0/1/0                unassigned      YES NVRAM  administratively down down
Serial0/1/1                unassigned      YES NVRAM  administratively down down

R1# show interfaces description
Interface                      Status         Protocol Description
Gi0/0                          up             up       LAN at Site 1
Gi0/1                          admin down     down
Se0/0/0                        up             up       link to R2
Se0/0/1                        admin down     down
Se0/1/0                        admin down     down
Se0/1/1                        admin down     down
```

Leased-Line WANs with PPP

Point-to-Point Protocol (PPP) plays the same role as HDLC: a data link protocol for use on serial links. However, HDLC was created for a world without routers. In contrast, PPP, defined in the 1990s, was designed with routers, TCP/IP, and other network layer protocols in mind, with many more advanced features.

This second major section of this chapter first discusses PPP concepts, including one example of a more advanced PPP feature (authentication). This section ends with some configuration examples using PPP.

PPP Concepts

PPP provides several basic but important functions that are useful on a leased line that connects two devices:

- Definition of a header and trailer that allows delivery of a data frame over the link
- Support for both synchronous and asynchronous links
- A protocol Type field in the header, allowing multiple Layer 3 protocols to pass over the same link
- Built-in authentication tools: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP)

- Control protocols for each higher-layer protocol that rides over PPP, allowing easier integration and support of those protocols

The next several pages take a closer look at the protocol field, authentication, and the control protocols.

PPP Framing

Unlike the standard version of HDLC, the PPP standard defines a protocol field. The protocol field identifies the type of packet inside the frame. When PPP was created, this field allowed packets from the many different Layer 3 protocols to pass over a single link. Today, the protocol Type field still provides the same function, usually supporting packets for the two different versions of IP (IPv4 and IPv6). Figure 13-12 shows the PPP framing, which happens to mirror the Cisco-proprietary HDLC framing that includes a protocol Type field (as shown earlier in Figure 13-9).

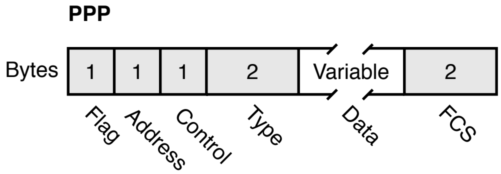


Figure 13-12 *PPP Framing*

PPP Control Protocols

In addition to HDLC-like framing, PPP defines a set of Layer 2 control protocols that perform various link control functions. The idea of these extra protocols works a little like how Ethernet includes additional protocols like Spanning Tree Protocol (STP). Ethernet has headers and trailers to deliver frames, plus it defines overhead protocols like STP to help make the frame forwarding process work better. Likewise, PPP defines the frame format in Figure 13-12, plus it defines other protocols to help manage and control the serial link.

PPP separates these control protocols into two main categories:

Key Topic

- **Link Control Protocol (LCP):** This one protocol has several different individual functions, each focused on the data link itself, ignoring the Layer 3 protocol sent across the link.
- **Network Control Protocols (NCP):** This is a category of protocols, one per network layer protocol. Each protocol performs functions specific to its related Layer 3 protocol.

The PPP LCP implements the control functions that work the same regardless of the Layer 3 protocol. For features related to any higher-layer protocols, usually Layer 3 protocols, PPP uses a series of PPP *control protocols* (CP), such as IP Control Protocol (IPCP). PPP uses one instance of LCP per link and one NCP for each Layer 3 protocol defined on the link. For example, on a PPP link using IPv4, IPv6, and Cisco Discovery Protocol (CDP), the link uses one instance of LCP plus IPCP (for IPv4), IPv6CP (for IPv6), and CDPCP (for CDP).

Table 13-4 summarizes the functions of LCP, gives the LCP feature names, and describes the features briefly. Following the table, the text explains one of the features, PPP authentication, in more detail. Later, the section “Implementing Multilink PPP” discusses the Multilink PPP (MLPPP) feature.

Table 13-4 PPP LCP Features

Function	LCP Feature	Description
Looped link detection	Magic number	Detects whether the link is looped, and disables the interface, allowing rerouting over a working route
Error detection	Link-quality monitoring (LQM)	Disables an interface that exceeds an error percentage threshold, allowing rerouting over better routes
Multilink support	Multilink PPP	Load balances traffic over multiple parallel links
Authentication	PAP and CHAP	Exchanges names and passwords so that each device can verify the identity of the device on the other end of the link

PPP Authentication

In networking, *authentication* gives one device a way to confirm that another device is truly the correct and approved device with which communications should occur. In other words, authentication confirms that the other party is the authentic other party, and not some imposter.

For instance, with PPP, if R1 and R2 are supposed to be communicating over a serial link, R1 might want R2 to somehow prove that the device claiming to be R2 really is R2. In that scenario, R1 wants to authenticate R2, with the authentication process providing a way for R2 to prove its identity.

WAN authentication is most often needed when dial lines are used. However, the configuration of the authentication features remains the same whether a leased line or dial line is used.

PPP defines two authentication protocols: PAP and CHAP. Both protocols require the exchange of messages between devices, but with different details. With PAP, the process works with the to-be-authenticated device starting the messages, claiming to be legitimate by listing a secret password in clear text, as shown in Figure 13-13.

Key Topic

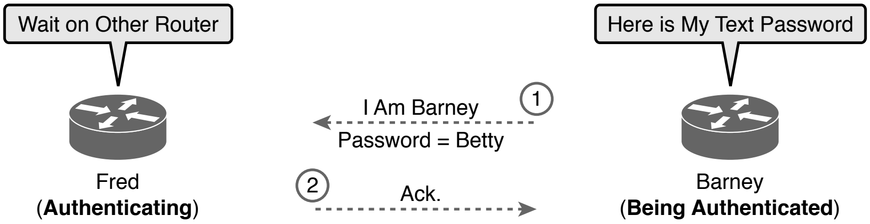


Figure 13-13 *PAP Authentication Process*

In the figure, when the link comes up, authentication takes two steps. At Step 1, Barney sends the shared password in clear text. Fred, who wants to authenticate Barney—that is, confirm that Barney is the real Barney—sees the password. Fred, configured with Barney's name and password, checks that configuration, confirming that it is the correct password, and sends back an acknowledgment that Barney has passed the authentication process.

CHAP, a much more secure option, uses different messages, and it hides the password. With CHAP, the device doing the authentication (Fred) begins with a message called a *challenge*, which asks the other device to reply. The big difference is that the second message in the flow (as shown in Figure 13-14) hides the authentication password by instead sending a hashed version of the password. Router Fred has been preconfigured with Barney's name and password in such a way that Fred can confirm that the hashed password sent by Barney is indeed the same password that Fred lists in his configuration for Barney. If the password is indeed the correct password, Fred sends back a third message to confirm the successful authentication of Barney.

Key Topic

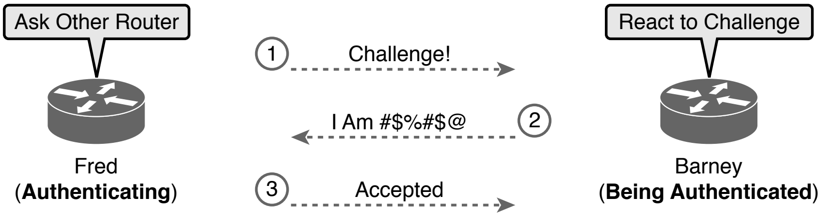


Figure 13-14 *CHAP Authentication Process*

Both Figures 13-13 and 13-14 show authentication flows when authentication works. When it fails (for instance, if the passwords do not match), a different final message flows. Also, if the authentication fails, PPP leaves the interface in an up/down state, and the router cannot forward and receive frames on the interface.

PAP flows are much less secure than CHAP because PAP sends the hostname and password in clear text in the message. These can be read easily if someone places a tracing tool in the circuit. CHAP instead uses a one-way hash algorithm, called message digest 5 (MD5), with input to the algorithm being a password that never crosses the link plus a shared random number.

The CHAP process also uses a hash value only one time so that an attacker cannot just make a copy of the hashed value and send it at a later date. To make that work, the CHAP challenge (the first CHAP message) states a random number. The challenged router runs the hash algorithm using the just-learned random number and the secret password as input, and sends the results back to the router that sent the challenge. The router that sent the challenge runs the same algorithm using the random number (sent across the link) and the password (as stored locally); if the results match, the passwords must match. Later, the next time the authentication process work occurs, the authenticating router generates and uses a different random number.

PAP and CHAP are a few examples of the work done by PPP's LCP. The next topic looks at how to configure and verify PPP.

Implementing PPP

Configuring PPP, as compared to HDLC, requires only one change: using the **encapsulation ppp** command on both ends of the link. As with HDLC, other items can be optionally configured, such as the interface **bandwidth**, and a **description** of the interface. And of course, the interface must be enabled (**no shutdown**). But the configuration to migrate from HDLC to PPP just requires the **encapsulation ppp** command on both routers' serial interfaces.

Example 13-4 shows a simple configuration using the two routers shown in Figure 13-11, the same internetwork used for the HDLC example. The example includes the IP address configuration, but the IP addresses do not have to be configured for PPP to work.

Example 13-4 *Basic PPP Configuration*

```
! The example starts with router R1
interface Serial0/0/0
 ip address 192.168.2.1 255.255.255.0
 encapsulation ppp
 clockrate 2000000
```

```
! Next, the configuration on router R2
interface Serial0/0/1
 ip address 192.168.2.2 255.255.255.0
 encapsulation ppp
```

The one **show** command that lists PPP details is the **show interfaces** command, with an example from R1 listed in Example 13-5. The output looks just like it does for HDLC up until the first highlighted line in the example. The two highlighted lines confirm the configuration ("Encapsulation PPP"). These lines also confirm that LCP has completed its work successfully, as noted with the "LCP Open" phrase. Finally, the output lists the fact that two CPs, CDPCP and IPCP, have also successfully been enabled—all good indications that PPP is working properly.

Example 13-5 *Finding PPP, LCP, and NCP Status with* **show interfaces**

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
! Lines omitted for brevity
```

Implementing PPP CHAP

The simplest version of CHAP configuration requires only a few commands. The configuration uses a password configured on each router. (As an alternative, the password could be configured on an external authentication, authorization, and accounting [AAA] server outside the router.)

To configure PPP along with CHAP on an interface that has all default configuration on the serial interfaces of both routers, follow these steps:

Config Checklist

Step 1. Use the **encapsulation ppp** command in interface configuration mode, on the serial interfaces on both routers, to enable PPP on the interfaces.

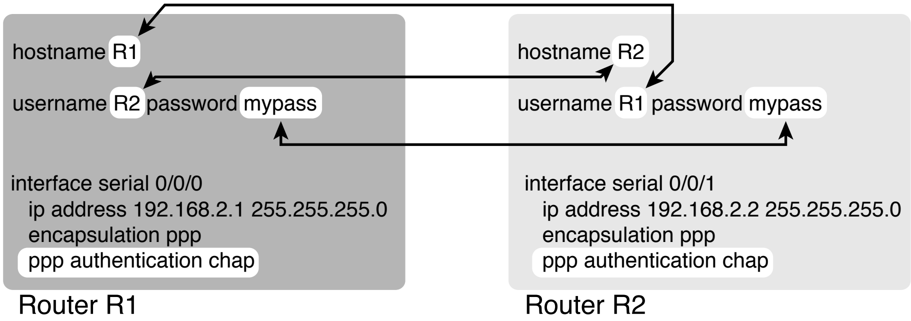
Step 2. Define the usernames and passwords used by the two routers:

A. Use the **hostname** *name* command in global configuration mode on each router, to set the local router's name to use when authenticating.

B. Use the **username** *name* **password** *password* command in global configuration mode on each router, to define the name (case-sensitive) used by the neighboring router, and the matching password (case-sensitive). (The name in the **username** command should match the name in the neighboring router's **hostname** command.)

Step 3. Use the **ppp authentication chap** command in interface configuration mode on each router to enable CHAP on each interface.

Figure 13-15 shows the configuration on both R1 and R2 to both enable PPP and add CHAP to the link. The figure shows how the name in the **hostname** command on one router must match the **username** command on the other router. It also shows that the password defined in each **username** command must be the same (mypass in this case).



```
hostname R1

username R2 password mypass

interface serial 0/0/0
  ip address 192.168.2.1 255.255.255.0
  encapsulation ppp
  ppp authentication chap
```

```
hostname R2

username R1 password mypass

interface serial 0/0/1
  ip address 192.168.2.2 255.255.255.0
  encapsulation ppp
  ppp authentication chap
```

Figure 13-15 *CHAP Configuration*

You can confirm that CHAP authentication has succeeded in a couple of ways. First, if CHAP authentication is enabled but CHAP authentication fails, the protocol status of the interface falls to a down state. To check that status, use the usual **show interfaces** [*type number*] command or **show interfaces status** command. Additionally, if CHAP is enabled but CHAP authentication fails, the **show interfaces** command does not list "LCP Open" as shown in this example. Example 13-6 lists the output of the **show interfaces serial0/0/0** command from R1, with CHAP enabled per Figure 13-15, with CHAP working. However, note that this command does not tell us whether authentication has been configured or not.

Example 13-6 *Confirming CHAP Authentication with* **show interfaces**

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
! Lines omitted for brevity
```

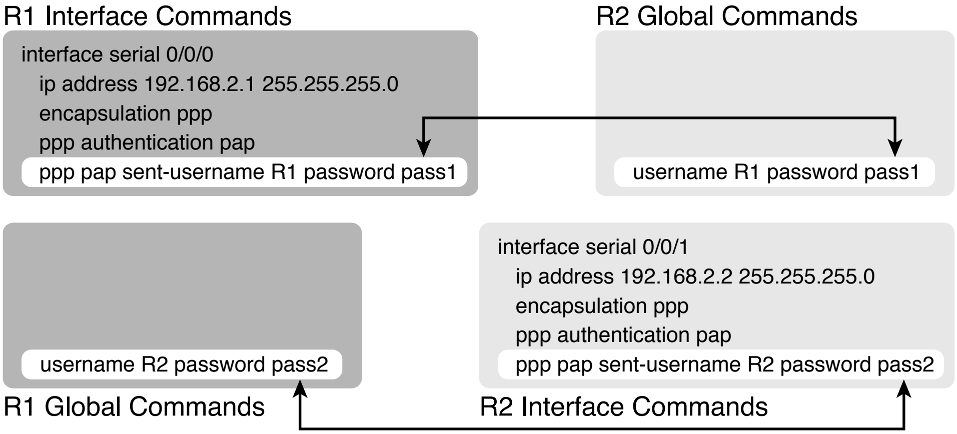
```
R1# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ -------------------- -------- --------------- --------------------
Se0/0/0      LCP+ CHAP+ IPCP+ CDP> LocalT   192.168.2.2     R2
```

The more obvious way to confirm that CHAP works is to use the **show ppp all** command, as shown at the end of Example 13-6. This command lists a single line per PPP connection in the router. The highlighted header in the example is the column where this command lists various PPP protocols and their status, with a plus sign (+) meaning that the listed protocol is OPEN, and a minus sign (–) meaning that the protocol has failed. The highlighted parts of this command in the example confirm that Serial0/0/0 uses PPP, with CHAP authentication, and that CHAP authentication worked (as proved by the OPEN status of the CHAP protocol).

Implementing PPP PAP

PAP configuration differs from CHAP configuration in a couple of ways. First, PAP uses the similar **authentication ppp pap** command instead of the **authentication ppp chap** command. Then, PAP configures the sent username/password pair much differently than CHAP. A router defines the username/password pair it will send using the **ppp pap sent-username** command, configured as an interface subcommand. Once sent, the other router receives that username/password pair, and compares those values with its various **username password** global commands. Figure 13-16 shows a completed configuration for two routers (R1 and R2), with emphasis on matching the **ppp pap sent-username** command on one router with the **username password** commands on the other router.

Key Topic



```
interface serial 0/0/0
  ip address 192.168.2.1 255.255.255.0
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username R1 password pass1
```

```
username R1 password pass1
```

```
username R2 password pass2
```

```
interface serial 0/0/1
  ip address 192.168.2.2 255.255.255.0
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username R2 password pass2
```

Figure 13-16 *PAP Configuration*

Example 13-7 now shows two commands used to verify PAP operation. In particular, note that the **show interfaces** command tells us nothing more and nothing less as compared to using CHAP authentication. The line protocol status being up confirms that authentication, if configured, worked. (However, nothing in the **show interfaces** command output tells us whether or not CHAP or PAP has been configured.) As with CHAP, the LCP status of Open also confirms that authentication worked, again assuming authentication is configured.

However, just as is the case when using CHAP, or when using no authentication at all, this command does not confirm whether authentication has been configured or, if it is configured, which authentication protocol is used. The better confirmation comes from the **show ppp all** command at the bottom of the example, which identifies PAP as configured on interface Serial0/0/0, and in this case the protocol is OPEN, meaning that authentication worked.

Example 13-7 *Configuring and Verifying PAP Authentication*

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
! Lines omitted for brevity
R1# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ --------------------- -------- --------------- --------------------
Se0/0/0      LCP+ PAP+ IPCP+ CDPC> LocalT   192.168.2.2     ciscouser2
```

Finally, note that you can configure the interface to try using the PAP process first, but if the other side does not support PAP, it then tries CHAP. You can configure to try PAP first or CHAP first. Just configure the commands to support both, and add the **ppp authentication pap chap** command to try PAP first, or the **ppp authentication chap pap** command to try CHAP first.

Implementing Multilink PPP

Network designers sometimes use multiple parallel serial links between two routers, rather than a single serial link. That motivation may be to improve availability, so if one link fails, at least the others are working. The motivation may be simple economics—it may be cheaper to install two or three parallel T1 lines (at about 1.5 Mbps each) rather than move up to the next faster type of line, a T3 line, using a fractional T3 service. Whatever the reasons, you end up with a design that looks like the design in Figure 13-17, with multiple serial links between two routers.

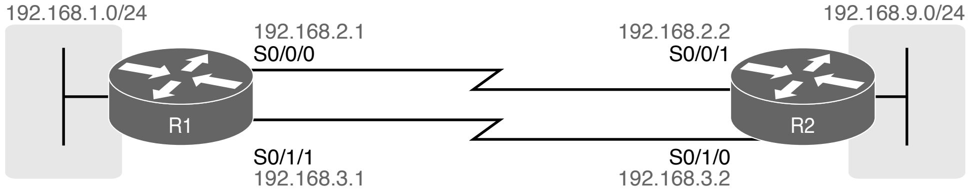


Figure 13-17 *Multiple Parallel Serial Links Between Routers*

If the network engineer configures the parallel serial links as discussed so far in this chapter, each link has IP addresses and can be used to forward IP packets. To make that happen, the interior routing protocol would run over each of the parallel links, with routing protocol neighbor relationships formed over each link. As a result, each router would learn multiple routes to every remote destination subnet—one such route for each parallel link.

Figure 13-18 shows the concept of having multiple equal-metric routes, one for each of the parallel serial links. It shows the same design as Figure 13-17, with two links. R1 has one route for network 192.168.9.0/24 over the top link, and one over the bottom link. If using EIGRP, R1 would have two EIGRP neighbor relationships with R2, one over each link.

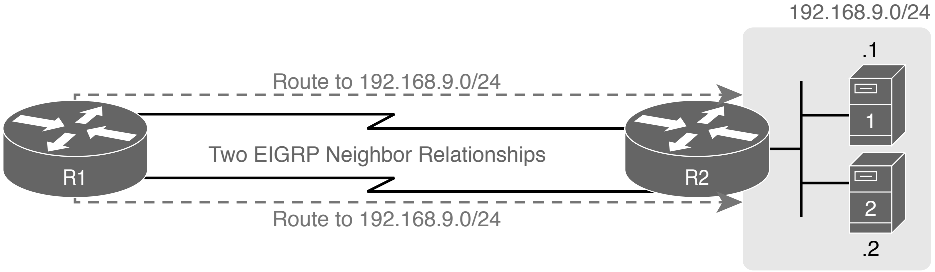


Figure 13-18 *Two IP Routes for One Network, One Per Parallel Serial Link*

The Layer 3 routing logic in Cisco IOS will then balance packets across the multiple links using the routes as shown in the figure. By default, IOS balances on a destination-by-destination address basis—for instance, in Figure 13-18, all packets to 192.168.9.1 might flow over the top link, with all packets going to destination address 192.168.9.2 being routed over the lower link. IOS can be configured to balance on a packet-by-packet basis.

Using the Layer 3 features discussed in the last page or so works, and works well in many cases. However, PPP offers a feature that simplifies the Layer 3 operations in topologies that use multiple parallel PPP links, with a feature called Multilink PPP (MLPPP).

Multilink PPP Concepts

Multilink PPP (MLPPP) is a PPP feature useful when using multiple parallel serial links between two devices. It provides two important features. First, it reduces the Layer 3 complexity by making the multiple serial interfaces on each router look like a single interface from a Layer 3 perspective. Instead of multiple subnets between routers, with multiple routing protocol neighbor relationships, and multiple equal-metric routes learned for each remote subnet, routers would have one subnet between routers, one routing protocol neighbor relationship, and one route per destination subnet. Figure 13-19 shows these main ideas for the same physical topology shown in Figure 13-18, which has multiple physical links.

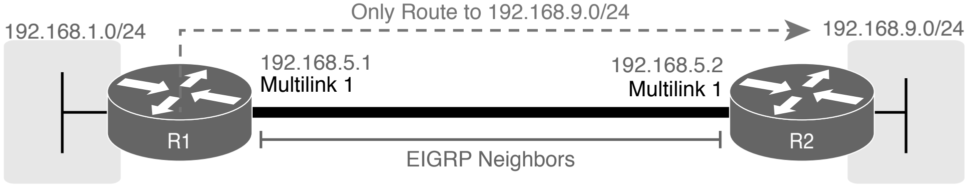


Figure 13-19 *Layer 3 Concept Created by Multilink Interface*

MLPPP makes the multiple physical links work like a single link by using a virtual interface called a multilink interface. The Layer 3 configuration (like IPv4 and IPv6 addresses and routing protocol interface subcommands) is added to the multilink interface. Then the configuration associates the physical serial interfaces with the multilink interface, connecting the Layer 2 logic that works with the multiple serial links with the Layer 3 logic that works on the single multilink interface.

In addition to simplifying Layer 3 details as just described, MLPPP balances the frames sent at Layer 2 over the multiple links. With MLPPP, a router's Layer 3 forwarding logic forwards each packet out the multilink interface. When IOS internally routes a packet out a multilink interface, MLPPP load-balancing logic takes over, encapsulating the packet into a new data link frame, and load balancing the frame.

Interestingly, MLPPP load balances the data link frame by fragmenting the frame into multiple smaller frames, one per active link, as shown with the process in Figure 13-20. Steps 1 and 2 show normal routing, with an encapsulated IP packet arriving at Step 1, and the router making the usual routing decision at Step 2. However, with the packet exiting a multilink interface, MLPPP fragments the packet into pieces (called fragments), with a PPP header/trailer around each, with a few extra header bytes to manage the fragmentation process. The receiving router reassembles the fragments back into the original packet (Step 4), with normal IP routing shown at Step 5.

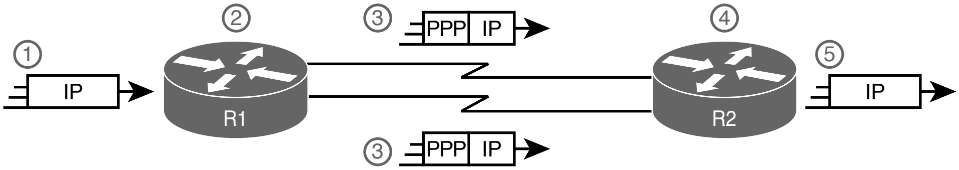


Figure 13-20 *Layer 2 Fragmentation to Balance Traffic over Multiple Links*

MLPPP's load-balancing process allows for some small variations in the sizes of the fragments, but for the most part, Cisco routers will balance the bytes sent equally across the active links in the multilink bundle. For instance, if three links are active, the router forwards about one-third of the byte volume of traffic.

Configuring MLPPP

Implementing MLPPP requires a longer configuration than most features discussed in this book. So first, to set the context a bit, think about these main three configuration requirements for MLPPP:

Key Topic

Step 1. Configure matching multilink interfaces on the two routers, configuring the interface subcommands for all Layer 3 features (IPv4, IPv6, and routing protocol) under the multilink interfaces (and not on the serial interfaces).

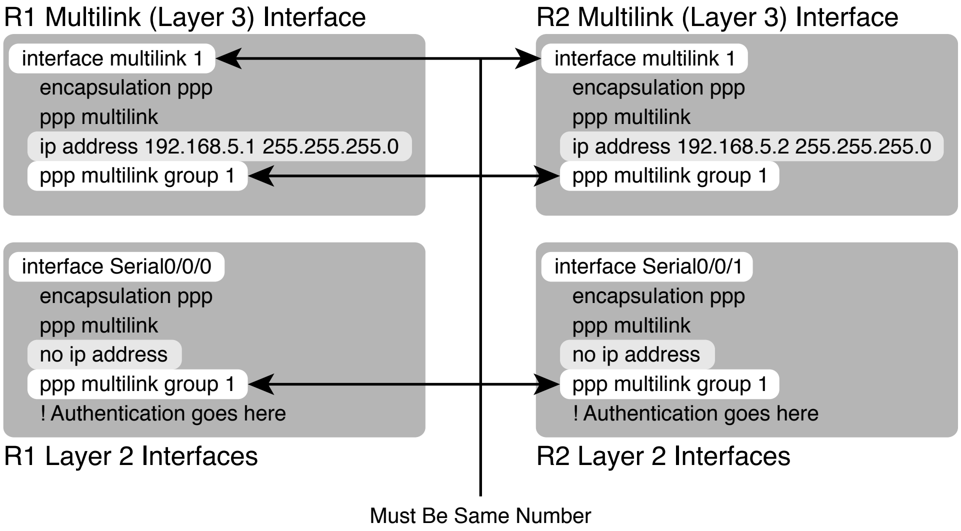
Step 2. Configure the serial interfaces with all Layer 1 and 2 commands, like **clock rate** (Layer 1) and **ppp authentication** (Layer 2).

Step 3. Configure some PPP commands on both the multilink and serial interfaces, to both enable MLPPP and associate the multilink interface with the serial interfaces.

Figure 13-21 shows all the specific MLPPP commands in a working example. The example is based on the design in Figures 13-19 and 13-20. Note that for space, Figure 13-21 shows the configuration for only one of the two serial interfaces, but all serial interfaces would have the same subcommands when used for MLPPP.

First, focus on the six configuration commands noted with white highlight boxes in Figure 13-21 as pointed to with arrows. The **interface multilink 1** command on each router creates the multilink interface on that router. The network engineer chooses the interface number, but the number must be the same on both routers, or the link will not work. Additionally, the multilink interfaces and the physical serial interfaces must all have both a **ppp multilink group 1** command, and they must all again refer to that same number (1 in this example). Any number in range could be used, but the number must match with the commands highlighted in the figure.

Key Topic


R1 Multilink (Layer 3) Interface
R2 Multilink (Layer 3) Interface
R1 Layer 2 Interfaces
R2 Layer 2 Interfaces
Must Be Same Number

```
interface multilink 1
  encapsulation ppp
  ppp multilink
  ip address 192.168.5.1 255.255.255.0
  ppp multilink group 1
```

```
interface multilink 1
  encapsulation ppp
  ppp multilink
  ip address 192.168.5.2 255.255.255.0
  ppp multilink group 1
```

```
interface Serial0/0/0
  encapsulation ppp
  ppp multilink
  no ip address
  ppp multilink group 1
  ! Authentication goes here
```

```
interface Serial0/0/1
  encapsulation ppp
  ppp multilink
  no ip address
  ppp multilink group 1
  ! Authentication goes here
```

Figure 13-21 *MLPPP Configuration*

Now look at the **ip address** commands. Note that the configuration shows IPv4 addresses configured on the multilink interfaces, but no IPv4 address at all on the serial interface. In short, the multilink interface has the Layer 3 configuration, and the serial interfaces do not. As a result, the routing and routing protocol logic will work with the multilink interface.

Finally, note that both the multilink and serial interfaces have two additional commands: **encapsulation ppp** (which enables PPP), and **ppp multilink** (which adds multilink support).

NOTE Figure 13-21 shows only one serial interface, but each serial interface in the multilink group would need the same configuration.

Verifying MLPPP

To verify that an MLPPP interface is working, it helps to think about the Layer 3 features separately from Layer 1 and Layer 2 details. For Layer 3, all the usual IPv4, IPv6, and routing protocol commands will now list the multilink interface rather than the physical serial interfaces. You can also just ping the IP address on the other end of the multilink to test the link. Example 13-8 shows a few commands to confirm the current working state of the MLPPP link, taken from the working configuration in Figure 13-21.

Example 13-8 *Verifying Layer 3 Operations with an MLPPP Multilink Interface*

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

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
      192.168.5.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.5.0/24 is directly connected, Multilink1
L        192.168.5.1/32 is directly connected, Multilink1
C        192.168.5.2/32 is directly connected, Multilink1
D     192.168.9.0/24 [90/1343488] via 192.168.5.2, 16:02:07, Multilink1

R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(1)
                   Xmit Queue   PeerQ        Mean   Pacing Time   Multicast    Pending
Interface    Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Mu1            1        0/0         0/0         1       0/8           50           0
Gi0/0          1        0/0         0/0         1       0/0           50           0

R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         192.168.1.1     YES manual up                    up
GigabitEthernet0/1         unassigned      YES manual up                    up
Serial0/0/0                unassigned      YES manual up                    up
Serial0/0/1                unassigned      YES manual administratively down down
Serial0/1/0                unassigned      YES NVRAM  administratively down down
Serial0/1/1                unassigned      YES NVRAM  up                    up
Multilink1                 192.168.5.1     YES manual up                    up
```

Working from the top of the example to the bottom, note that the IPv4 routing table lists interface multilink 1 as the outgoing interface in a variety of routes. However, the two serial interfaces are not listed at all, because they do not have IP addresses and the router's routing logic works with the multilink interface instead. Similarly, the **show ip eigrp interfaces** command lists interfaces on which EIGRP is enabled, listing Mu1 (Multilink 1), and not listing either of the two serial interfaces in the MLPPP bundle. Finally, note that the **show ip interface brief** command does list both the serial interfaces and the multilink interface, but the output confirms that no IP address has been configured on the serial interfaces, as noted with the "unassigned" text under the IP-Address column.

Each multilink interface has a line and protocol status like any other interface, and if that status is up/up, IOS believes the multilink interface is working. By default, that working state implies that at least one of the physical links in the MLPPP group is also working—that is, some of the physical links can fail, and the multilink stays up. You can always directly verify the serial interfaces in the multilink group with the same commands discussed earlier in the chapter (**show controllers**, **show interfaces**). Additionally, the two commands in Example 13-9 give some insight into the specifics of MLPPP operation.

Example 13-9 *Verifying Operational Details of an MLPPP Group*

```
R1# show interfaces multilink 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 192.168.5.1/24
  MTU 1500 bytes, BW 3088 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
! lines omitted for brevity

R1# show ppp multilink

Multilink1
  Bundle name: R2
  Remote Username: R2
  Remote Endpoint Discriminator: [1] R2
  Local Username: R1
  Local Endpoint Discriminator: [1] R1
  Bundle up for 16:50:33, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 96 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x654D7 received sequence, 0x654D5 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 16:50:33
    Se0/0/0, since 16:23:16
No inactive multilink interfaces
```

First, notice that the **show interfaces multilink 1** command lists many familiar details and some mentions about multilink. In particular, the output shows the traditional line and protocol status, both in an up state, meaning that the interface is working. On the sixth line, the output mentioned a working multilink state of "Open" in the section about PPP control protocols, confirming that MLPPP is in effect.

Finally, the output of the **show ppp multilink** command identifies the links configured in each multilink bundle, as well as which ones are active. In this case, on R1, interfaces S0/0/0 and S0/1/1 are active, as highlighted at the bottom of the example. The timer to the side shows that both have been active a little over 16 hours. Seeing these two interfaces in the list confirms not only that the physical interfaces are working, but that the MLPPP configuration includes both of these links in multilink group 1.

Troubleshooting Serial Links

This final major section discusses how to isolate and find the root cause of problems related to topics covered earlier in this chapter. Also, this section does not attempt to repeat the IP troubleshooting coverage in Part II of this book, but it does point out some of the possible symptoms on a serial link when a Layer 3 subnet mismatch occurs on opposite ends of a serial link, which prevents the routers from routing packets over the serial link.

A simple **ping** command can determine whether a serial link can or cannot forward IP packets. A ping of the other router's serial IP address—for example, a working **ping 192.168.2.2** command on R1 in Figure 13-11, the figure used for both the HDLC and PPP configuration examples—proves that the link either works or does not.

If the **ping** does not work, the problem could be related to functions at Layer 1, 2, or 3. The best way to isolate which layer is the most likely cause is to examine the interface status codes described in Table 13-5.

Table 13-5 Interface Status Codes and Typical Meanings When a Ping Does Not Work

Line Status	Protocol Status	Likely General Reason/Layer
Administratively down	Down	Interface shutdown
Down	Down	Layer 1
Up	Down	Layer 2
Up	Up	Layer 3

The serial link verification and troubleshooting process should begin with a simple three-step process:

Step 1. From one router, ping the other router's serial IP address.

Step 2. If the ping fails, examine the interface status on both routers and investigate problems related to the likely problem areas listed in Table 13-5.

Step 3. If the ping works, also verify that any routing protocols are exchanging routes over the link, as discussed in Chapter 11, "Troubleshooting IPv4 Routing Protocols."

NOTE The interface status codes can be found using the **show interfaces**, **show ip interface brief**, and **show interfaces description** commands.

The rest of this section explores the specific items to be examined when the ping fails, based on the combinations of interface status codes listed in Table 13-5.

Troubleshooting Layer 1 Problems

The interface status codes, or interface state, play a key role in isolating the root cause of problems on serial links. In fact, the status on both ends of the link may differ, so it is important to examine the status on both ends of the link to help determine the problem.

For example, a serial link fails when just one of the two routers has administratively disabled its serial interface with the **shutdown** interface subcommand. When one router shuts down its serial interface, the other router sits in a down/down state (line status down, line protocol status down), assuming the second router's interface is not also shut down. The solution is to just configure a **no shutdown** interface configuration command on the interface.

A serial interface with a *down* line status on both ends of the serial link—that is, both ends in a down/down state—usually points to some Layer 1 problem. Figure 13-22 summarizes the most common causes of this state. In the figure, R2's serial interface has no problems at all; the center and left side of the figure show common root causes that then result in R2's serial interface being in a down/down state.

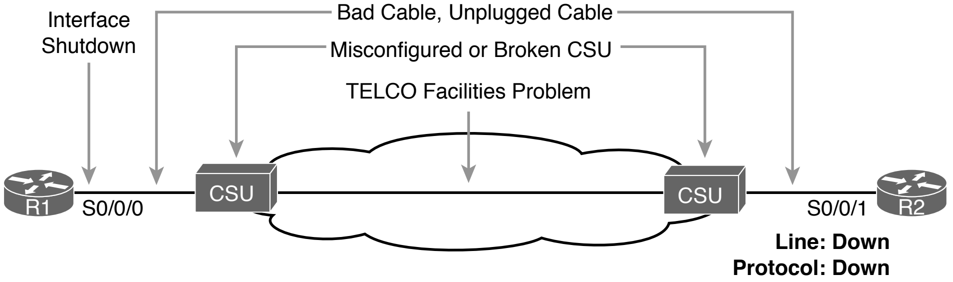


Figure 13-22 *Problems That Result in a Down/Down State on Router R2*

Troubleshooting Layer 2 Problems

Data link layer problems on serial links usually result in at least one of the routers having a serial interface status of up/down. In other words, the line status (the first status code) is up, while the second status (the line protocol status) is down. Table 13-6 lists some of these types of problems.

Table 13-6 Likely Reasons for Data Link Problems on Serial Links

Line Status	Protocol Status	Likely Reason
Up	Down on both ends[1]	Mismatched **encapsulation** commands
Up	Down on one end, up on the other	Keepalive disabled on the end in an up state when using HDLC
Up	Down on both ends	PAP/CHAP authentication failure

[1] In this case, the state may flap from up/up, to up/down, to up/up, and so on, while the router keeps trying to make the encapsulation work.

The first of these problems—a mismatch between the configured data link protocols—is easy to identify and fix. The **show interfaces** command lists the encapsulation type on about the seventh line of the output, so using this command on both routers can quickly identify the problem. Alternatively, a quick look at the configuration, plus remembering that HDLC is the default serial encapsulation, can confirm whether the encapsulations are mismatched. The solution is simple: Reconfigure one of the two routers to match the other router's **encapsulation** command.

The other two root causes require a little more discussion to understand the issue and determine if they are the real root cause. The next two sections take a closer look at each.

Keepalive Failure

The router *keepalive* feature helps a router notice when a link is no longer functioning. Once a router believes the link no longer works, the router can bring down the interface, allowing the routing protocol to converge to use other routes it they exist.

The keepalive function on an interface causes routers to send keepalive messages to each other every keepalive interval, defaulting to 10 seconds. For instance, on a serial link between R1 and R2, R1 sends a keepalive message every 10 seconds, and R2 expects to receive those keepalive messages every 10 seconds. If R2 fails to receive the keepalive messages for a set number of consecutive keepalive intervals (usually three or five intervals), R2 believes R1 has failed, and R2 changes the link to an up/down state. The keepalive process happens in both directions as well—R1 sends keepalives with R2 expecting to receive them, and R2 sends keepalives with R1 expecting to receive them.

A keepalive mismatch occurs when one router has keepalives enabled and one router does not. That combination is a mistake, and should not be used. Note that this keepalive mismatch mistake only breaks HDLC links; the PPP keepalive feature prevents the problem. Figure 13-23 shows one such example with HDLC and with R1 mistakenly disabling keepalives.

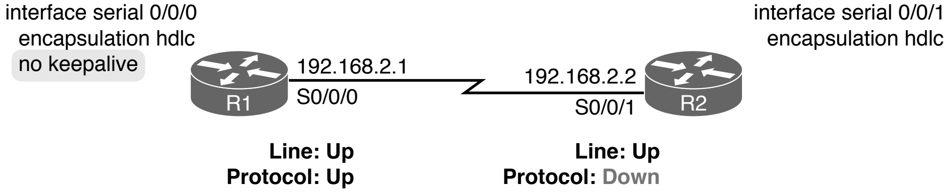


Figure 13-23 *Results when Using HDLC with a Keepalive Mismatch*

Note that the router interface that disables keepalives remains in an up/up state. In the scenario shown in Figure 13-23, R2's interface fails because

- R1 does not send keepalive messages, because keepalives are disabled.
- R2 still expects to receive keepalive messages, because keepalives are enabled.

You can verify the keepalive setting by looking at the configuration or by using the **show interfaces** command. The examples in this chapter list several examples of the **show interfaces** command that happen to list the text "Keepalive set (10 second)," meaning that keepalives are enabled with a 10-second interval. R1 would list the text "Keepalive not set" in this case.

PAP and CHAP Authentication Failure

As mentioned earlier, a failure in the PAP/CHAP authentication process results in both router interfaces failing to an up and down state. As shown in Examples 13-6 and 13-7, you can use the **show interfaces** and **show ppp all** commands to look further into the status of the PPP authentication process. By doing so, you can isolate and discover the root cause of why the interface is in an up/down state, ruling out or ruling in PPP authentication as the root cause.

Another deeper method to troubleshoot PPP authentication problems uses the **debug ppp authentication** command.

CHAP uses a three-message exchange, as shown back in Figure 13-14, with a set of messages flowing for authentication in each direction by default. If you enable the debug, shut down the link, and bring it back up, you will see debug messages that match that three-way exchange. If authentication fails, you see a failure message at the point at which the process fails, which may help you decide what specifically needs to be fixed.

Example 13-10 shows the three related debug messages when a link comes up. The network connects R1's S0/0/0 to router R2. The example extracts the three related debug messages from what would be a few dozen debug messages, so you would have to look for these. However, the output highlights the important parts of the process as seen back in Figure 13-14, as follows:

1. The "O" refers to output, meaning that this local router, R1, has output (sent) a Challenge message. Note the "from R1" at the end of the debug message, stating who the message is from.
2. The "I" refers to input, meaning that this local router, R1, has input (received) a Response message. Note the "from R2" at the end of the line.
3. The "O FAILURE" refers to R1 sending out a Failure message, telling R2 that the authentication process failed.

Example 13-10 *Debug Messages on Router R1 Confirming the Failure of CHAP*

```
R1# debug ppp authentication
PPP authentication debugging is on
! Lines omitted for brevity
*Nov 18 23:45:48.820: Se0/0/0 CHAP: O CHALLENGE id 1 len 23 from "R1"
*Nov 18 23:45:48.820: Se0/0/0 CHAP: I RESPONSE id 1 len 23 from "R2"
*Nov 18 23:45:48.820: Se0/0/0 CHAP: O FAILURE id 1 len 25 msg is "Authentication
  failed"
```

While using a **debug** command may tell us something about the problem, it does not always point to the specific command that is misconfigured. In this case, the fact that both routers send at least one CHAP message implies that both router interfaces can send frames, and that they have enabled CHAP. It looks more like R1 has rejected the hashed password supplied by R2. Note that this example was built by changing the **username** command to have an incorrect password, so that the CHAP process worked but the authentication was rejected.

Troubleshooting Layer 3 Problems

This chapter suggests that the best starting place to troubleshoot serial links is to ping the IP address of the router on the other end of the link—specifically, the IP address on the serial link. Interestingly, the serial link can be in an up and up state but the ping can still fail because of Layer 3 misconfiguration. In some cases, the ping may work but the routing protocols might not be able to exchange routes. This short section examines the symptoms, which differ slightly depending on whether HDLC or PPP is used and the root cause.

First, consider an HDLC link on which the physical and data link details are working fine. In this case, both routers' interfaces are in an up and up state. However, if the IP addresses configured on the serial interfaces on the two routers are in different subnets, a ping to the IP address on the other end of the link will fail because the routers do not have a matching route. For example, consider an example with a working HDLC link with the IP addresses shown earlier in Figure 13-23. Then, if R1's serial IP address remained 192.168.2.1, and R2's was changed to 192.168.3.2 (instead of 192.168.2.2), still with a mask of /24, the two routers would have connected routes to different subnets. They would not have a route matching the opposite router's serial IP address.

Finding and fixing a mismatched subnet problem with HDLC links is relatively simple. You can find the problem by doing the usual first step of pinging the IP address on the other end of the link and failing. If both interfaces have a status of up/up, the problem is likely this mismatched IP subnet.

For PPP links with the same IP address/mask misconfiguration, the ping to the other router's IP address actually works. However, the IP subnet mismatch still prevents EIGRP and OSPF neighbor relationships from forming, so it is still a good idea to follow the rules and put both serial interface IP addresses in the same subnet.

PPP makes the ping work with the mismatched subnet by adding a host route, with a /32 prefix length, for the IP address of the other router. Example 13-11 shows the working PPP link with addresses in different subnets.

NOTE A route with a /32 prefix, representing a single host, is called a *host route*.

Example 13-11 *PPP Allowing a Ping over a Serial Link, Even with Mismatched Subnets*

```
R1# show ip route
! Legend omitted for brevity
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
      192.168.3.0/32 is subnetted, 1 subnets
C        192.168.3.2 is directly connected, Serial0/0/0

R1# ping 192.168.3.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

The first highlighted line in the example shows the normal connected route on the serial link, for network 192.168.2.0/24. R1 thinks this subnet is the subnet connected to S0/0/0 because of R1's configured IP address (192.168.2.1/24). The second highlighted line shows the host route created by PPP, specifically for R2's new serial IP address (192.168.3.2). (R2 will have a similar route for 192.168.2.1/32, R1's serial IP address.) So, both routers have a route to allow them to forward packets to the IP address on the other end of the link, even though the other router's address is in a different subnet. This extra host route allows the ping to the other side of the serial link to work in spite of the addresses on each end being in different subnets.

Table 13-7 summarizes the behavior on HDLC and PPP links when the IP addresses on each end do not reside in the same subnet but no other problems exist.

Table 13-7 Summary of Symptoms for Mismatched Subnets on Serial Links

Symptoms When IP Addresses on a Serial Link Are in Different Subnets	HDLC	PPP
Does a ping of the other router's serial IP address work?	No	Yes
Can routing protocols exchange routes over the link?	No	No

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 13-8 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 13-8 Chapter Review Tracking

Review Element	Review Date(s)	Resource Used
Review key topics		Book, DVD/website
Review key terms		Book, DVD/website
Repeat DIKTA questions		Book, PCPT
Do labs		Blog
Review memory tables		Book, DVD/website
Review config checklists		Book, DVD/website
Review command tables		Book

Review All the Key Topics

Key Topic

Table 13-9 Key Topics for Chapter 13

Key Topic Element	Description	Page Number
Table 13-3	Speeds for WAN links per the T-carrier system	334
Figure 13-7	Role of the CSU/DSU and the router as DCE and DTE	335
List	PPP features	340
List	Comparison of PPP LCP and NCP	341
Figure 13-13	Example of messages sent by PAP	342
Figure 13-14	Example of messages sent by CHAP	343
Figure 13-16	Sample PAP configuration	346
List	MLPPP major configuration concepts	349
Figure 13-21	Sample MLPPP configuration	350

Key Terms You Should Know

leased line, telco, serial link, WAN link, T1, DS0, DS1, T3, customer premises equipment, CSU/DSU, serial cable, DCE, DTE, HDLC, PPP, CHAP, PAP, IP Control Protocol, keepalive, Link Control Protocol, Multilink PPP

Command References

Tables 13-10 and 13-11 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 13-10 Chapter 13 Configuration Command Reference

Command	Description
encapsulation {**hdlc** | **ppp**}	Interface subcommand that defines the serial data-link protocol
[**no**] **shutdown**	Administratively disables (**shutdown**) or enables (**no shutdown**) the interface in whose mode the command is issued
clock rate *speed*	Serial interface subcommand that, when used on an interface with a DCE cable, sets the clock speed in bps
bandwidth *speed-kbps*	Interface subcommand that sets the router's opinion of the link speed, in kilobits per second, but has no effect on the actual speed
description *text*	Interface subcommand that can set a text description of the interface
ppp authentication {**pap** | **chap**}	Interface subcommand that enables only PAP or only CHAP authentication
username *name* **password** *secret*	Global command that sets the password that this router expects to use when authenticating the router with the listed hostname
ppp pap sent-username *name* **password** *secret*	Interface subcommand that defines the username/password pair sent over this link when using PAP authentication

13

Command	Description
interface multilink *number*	Creates a multilink interface and moves the user to interface configuration mode on that interface
ppp multilink	Interface subcommand that enables MLPPP features
ppp multilink group *number*	Interface subcommand that associates the interface with a particular multilink interface and multilink group

Table 13-11 Chapter 13 EXEC Command Reference

Command	Description
show interfaces [*type number*]	Lists statistics and details of interface configuration, including the encapsulation type
show interfaces [*type number*] **description**	Lists a single line per interface (or if the interface is included, just one line of output total) that lists the interface status and description
show ip interface brief	Lists one line of output per interface, with IP address and interface status
show controllers serial *number*	Lists whether a cable is connected to the interface, and if so, whether it is a DTE or DCE cable
show ppp multilink	Lists detailed status information about each of the PPP multilink groups configured on the router
show ppp all	Lists one line of status information per PPP link on the router, including the status for each control protocol
debug ppp authentication	Generates messages for each step in the PAP or CHAP authentication process
debug ppp negotiation	Generates **debug** messages for the LCP and NCP negotiation messages sent between the devices

Index

Symbols

- **2-way state (neighbor relationships), 186, 628**
- **3G wireless, 393**
- **4G wireless, 393**
- **802.1D STP, 58, 62**
- **802.1Q, 20-21**
  - headers, 500-501
  - trunking. *See* ROAS
- **802.1w RSTP**
  - defined, 58
  - port roles, 60
  - port states, 62
- **802.11 headers, 501**

A

- **aaa authentication login default command, 149**
- **aaa new-model command, 149**
- **AAA servers**
  - authentication
    - *configuration, 148-150*
    - *login authentication rules, 150*
    - *login process, 147*
    - *TACACS+/RADIUS protocols, 148*
  - configuring for 802.1x, 145
  - defining, 149
  - enabling, 149
  - username/passwords, verifying, 145
- **aaS (as a Service), 742**
- **ABR (Area Border Router), 190, 625**
  - interface OSPF areas, verifying, 210-211
  - OSPFv2 multiarea configuration, 209-210
  - OSPFv3 multiarea configuration, 625
- **access**
  - Internet, 389
    - *cable Internet, 391*
    - *DSLs (digital subscriber lines), 390-391*
    - *fiber, 393*
    - *WANs, 389*
    - *wireless WANs, 392-393*
  - IPv6 restrictions, 685
  - public cloud services
    - *Internet, 745-746*
    - *private WANs, 746-749*
    - *VPNs, 747*
  - securing with IEEE 802.1x, 144-146
    - *AAA servers, configuring, 145*
    - *authentication process, 145*
    - *EAP, 146*
    - *switches as 802.1x authenticators, 145*
    - *username/password combinations, verifying, 145*
- **access-class command, 486**

access control lists. *See* ACLs

Access Control Server (ACS), 147

access interfaces, 24, 113-114

access layer switches, 156-157

access links

MetroE, 365

MPLS, 378

access-list command, 445, 457, 463-466, 486

building ACLs with, 454

examples and logic explanations, 467

extended numbered ACL configuration commands, 467

keywords

any, 448

deny, 448-449

log, 452

permit, 445, 448-449

tcp keyword, 464

upd keyword, 464

reverse engineering from ACL to address range, 454-456

ACI (Application Centric Infrastructure), 773-774

ACLs (access control lists), 586

ACL Analysis tool, 777-778

classification, 497

comparison of ACL types, 442-443

extended numbered ACLs

configuration, 467-470

matching protocol, source IP, and destination IP, 463-464

matching TCP and UDP port numbers, 464-467

overview, 462

GRE tunnel issues, 409-410

HSRP packets, blocking, 563

implementation considerations, 476-477

IPv4, 666-667

IPv6, 664-666

access-list commands, building, 678-679

access restrictions, 685

blocking, 683

capabilities, 669

extended, 674-678

filtering ICMPv6 NDP messages, 679-683

filtering policies, 668

ICMPv6 message filtering, 668-669

implicit filtering ICMPv6 NDP messages, 683-684

IPv4 ACL, compared, 666-667

limitations, 669-670

logging, 670

management control, 685

prefix lengths, 670

problems, 612

router originated packets, 670

standard, configuring, 671-674

testing, 677

tunneled traffic matching, 670

location and direction, 440-441

matching packets, 441-442

named ACLs

configuration, 472

editing, 473-475

overview, 471-472

numbered ACLs, 475-476

overview, 440

QoS tools, compared, 496

SNMP security, 698

- standard numbered ACLs
  - *access-list command, 454*
  - *command syntax, 445*
  - *configuration examples, 448-452*
  - *list logic, 444-445*
  - *matching any/all addresses, 448*
  - *matching exact IP address, 445-446*
  - *matching subset of address, 446-447*
  - *overview, 443*
  - *reverse engineering from ACL to address range, 454-456*
  - *troubleshooting, 452-453*
  - *verification, 452-453*
  - *wildcard masks, 446-448*
- troubleshooting, 477
  - *ACL behavior in network, 477-479*
  - *ACL interactions with router-generated packets, 483-485*
  - *commands, 479-480*
  - *common syntax mistakes, 481*
  - *inbound ACL filters routing protocol packets, 481-482*
  - *reversed source/destination IP address, 480-481*

ACL Analysis tool, 777-778

ACS (Access Control Server), 147

active HSRP routers, 558

address blocks. ***See*** **prefixes**

addresses
- families, 619
- global unicast, 593
- IPv4, 197
- IPv6
  - *assigning to hosts, 595-597*
  - *connectivity, verifying, 600-603*
  - *multicast, 682*
  - *router configuration, 598-599*
  - *static route configuration, 599*
  - *unicast, 593-595*
- link, 311-312
- link-local, 595
- MAC, 49
- public cloud assignment services, 756-757
- source/destination, 406
- unique local unicast, 593

adjacent neighbors, 186, 633

administrative distance, 177-178

administratively shutdown interfaces, 49

ADSL (asymmetric DSL), 391

advertising
- BGP routes, 303-304
- eBPG enterprise public prefixes, 307-308
- subnets to ISPs, 318

AF (Assured Forwarding), 502-503

agents (SNMP), 695
- Get/Set messages, 696
- MIB, 697
- NMS polling, 696
- notifications, 696-697

algorithms
- Dijkstra SPF, 180
- DUAL (Diffusing Update Algorithm), 242-243, 646
- IGP routing protocol algorithm, 175
- SPF (Shortest Path First), 180, 186-188
- STA (spanning-tree algorithm), 48

all IP addresses, matching, 448

alternate ports, 60-61, 91-92

Amazon Web Services (AWS), 742

American Registry for Internet Numbers (ARIN), 174

analyzers (network), 719

answering exam questions, 790-792

anti-replay (Internet VPNs), 394

any keyword, 448

any/all IP addresses, matching, 448

APIs (application programming interfaces), 768-769

APIC (Application Policy Infrastructure Controller), 774

APIC EM (APIC Enterprise Module), 774-776

- ACL Analysis tool, 777
- controller, 777
- labs website, 777
- Path Trace ACL Analysis tool, 777-778
- Path Trace app, 777

Application Centric Infrastructure (ACI), 773-774

Application Policy Infrastructure Controller (APIC), 774

application signatures, 498

application-specific integrated circuit (ASIC), 765

architectures (SDN), 770

- APIC Enterprise Module (APIC-EM), 774-776
  - *controller, 777*
  - *labs website, 778*
  - *Path Trace ACL Analysis tool, 777-778*
  - *Path Trace app, 777*
- Application Centric Infrastructure (ACI), 773-774
- comparisons, 776
- Open SDN, 771
- Open SDN Controller (OSC), 772
- OpenDaylight (ODL), 771-772
- OpenFlow, 771

Area Border Router. ***See*** **ABR**

area design (OSPF), 189-190

- ABR, 190, 210-211
- areas, 189-190
- backbone areas, 190
  - *multiarea on ABR configuration, 625*
  - *super, 381*
- backbone routers, 190
- benefits, 191
- interarea routes, 190
- internal routers, 190
- intra-area routes, 190
- mismatches, finding, 290-291
- MPLS VPNs, 381-382
- network size, 189
- problems, 188, 281
- single-area, 188
- SPF workload, reducing, 190
- three-area, 189

ARIN (American Registry for Internet Numbers), 174

AS (autonomous system), 174, 304

as a Service (-aaS), 742

ASAv (virtual ASA firewall), 754

ASIC (application-specific integrated circuit), 765

ASNs (AS numbers), 174

- BGP, 304
- EIGRP, 248
  - *for IPv6, 649*
  - *neighbors, 235, 288*

Assured Forwarding (AF), 502-503

asymmetric DSL (ADSL), 391

attacks
DHCP-based, 152
types, 150
auth keyword (snmp-server group command), 707
authentication
802.1x, 145
AAA servers
configuration examples, 148-150
login authentication rules, 150
login process, 147
TACACS+/RADIUS protocols, 148
EIGRP neighbors, 235, 286
Internet VPNs, 393
PPP, 342-343
PPP CHAP, 356
PPP PAP, 356
SNMPv3, 699, 707-708
authentication ppp pap command, 346
authenticators, switches as, 145
auto-cost reference-bandwidth command, 222, 643
autonomous system (AS), 174, 304
auto-summary command, 267
defined, 270
EIGRP, 247
EIGRP for IPv4, 648
autosummarization, 266
classful network boundaries, 266-267
discontiguous classful networks, 267-268
AWS (Amazon Web Services), 742

B

backbone areas (OSPF), 190
multiarea on ABR configuration, 625
super, 381
backbone routers, 190
backup DRs (BDRs), 185, 211-212
backup port role (RSTP), 62-63
backup ports, 60, 91-92
bandwidth
EIGRP
for IPv6 routes, 650-651
metrics, 237-239, 265
routes, tuning, 259
interfaces
defaults, 216
higher, 217
OSPF costs based on, 216-217
least-bandwidth, 237
managing, 491
MetroE, 373-374
reference, 216-217
bandwidth command, 216, 359
defined, 222, 270
EIGRP, 247, 647
for IPv6, 662
metrics, 237, 265
OSPFv3 interface, 643
batch traffic, 493
BDRs (backup DRs), 185, 211-212
Bellman-Ford protocols. ***See*** **DV protocols**
best path selection (BGP), 305-306
BGP (Border Gateway Protocol), 174, 300, 303
AS, 304
ASNs, 304

best path selection, 305-306
configuring, 310
external. *See* eBGP
IGPs, compared, 302
internal (iBGP), 304
ISP default routes, learning, 320-321
neighbors, 303
disabling, 314
states, 313
prefixes, 303
reachability, 302
route advertising, 303-304
routing table analysis reports website, 303
table entries, injecting, 314
advertising subnets to ISPs, 318
classful network routes, 315-318
static discard routes, 319-320
update messages, 303-310

bgp commands, 311

BIDs (bridge IDs)
STP, 49
root switch election, 50-52
verification, 77
system ID extensions, 73-74

binary-to-hexadecimal conversion, 808

binary wildcard masks, 447

blocking state
interfaces, 47-49
RSTP ports, 92

Border Gateway Protocol. *See* BGP

BPDUs (bridge protocol data units), 49

BPDU Guard, 66
configuring, 81
enabling/disabling, 83
global settings, displaying, 83
verifying, 82-83

branch offices public cloud example, 749-752
email services traffic flow, 750-751
Internet connections, 751
private WAN connections, 751

bridge IDs. *See* BIDs

bridges. *See* switches

broadcast storms, 45-47

burned-in MAC addresses, 49

C

cable Internet, 391

cabling
DTE cables, 335
leased-line WANs, 332-333
stacking cables, 156

CAC (Call Admission Control) tools, 507

carrier Ethernet, 366

Catalyst switches RSTP modes, 88-90

Catalyst switches STP modes, 88-89

CBWFQ (Class-Based Weighted Fair Queuing), 505

***CCENT/CCNA ICND1 100-105 Official Cert Guide*, 272**

***CCNA ICND2 200-105 Official Cert Guide Premium Edition eBook and Practice Test*, 792**

CCNA ICND2 Config Labs website, 796

***CCNA Routing and Switching ICND2 Official Cert Guide website*, 777**

CCNA R&S practice exam, 790

CE (customer edge), 377

centralized control planes, 766

CFN (Cisco Feature Navigator), 531

challenge messages, 342

channel-group command (EtherChannels), 84, 95, 543
incorrect options, troubleshooting, 106-108
Layer 3, troubleshooting, 541
channel service unit (CSU)/data service unit (DSU), 332-334
CHAP (Challenge-Handshake Authentication Protocol)
authentication, 342, 356
configuring, 344-345
verifying, 345-346
chassis aggregation, 159
benefits, 161
design, improving, 160
distribution/core switches high availability, 159-160
switch stacking, 159-161
CIR (committed information rate), 373, 509
Cisco
Access Control Server (ACS), 147
Application Centric Infrastructure (ACI), 773-774
BPDU Guard, 66
Catalyst switches RSTP modes, 88-90
Catalyst switches STP modes, 88-89
DevNet, 777
Feature Navigator (CFN), 531
Intercloud Fabric, 749
nondisclosure agreement (NDA), 788
Open SDN Controller (OSC), 772
Prime management products website, 695
server hardware, 732-733
Unified Communication Manager (CUCM), 35
virtual ASA firewall (ASAv), 754
Class-Based Weighted Fair Queuing (CBWFQ), 505
Class of Service (CoS) fields (802.1Q header), 500-501
Class Selector (CS), 503
classful networks
autosummarization at boundaries, 266-267
discontiguous, 267-268
routes, injecting, 315-318
classful routing protocols, 177, 266
classic mode (EIGRP configuration), 249
classification (QoS), 495
ACLs, 497
matching, 496-497
NBAR, 498
router queuing, 496
routers, 497
with marking, 497
classless routing protocols, 177
clear ip ospf process command, 204, 223
clear-text passwords, 698
CLI skills, 794-796
client VPNs, 396-397
clock rate commands, 349, 359
clocking, 332
cloud computing
address assignment services, 756-757
cloud services catalogs, 740
Cloud Services Routers (CSRs), 747
DHCP services, 757
Infrastructure as a Service (IaaS), 742
NTP, 757-758
Platform as a Service (PaaS), 743-744
private, 739-741

public, 741

accessing with Internet, 745-746

accessing with private VPNs, 747

accessing with private WANs, 746-749

branch offices example, 749-752

DNS services, 754-756

email services traffic flow, 750-751

intercloud exchanges, 748-749

Internet connections, 751

private WAN connections, 751

VNFs, 752-754

services, 739

Software as a Service (SaaS), 743

Cloud Services Routers (CSRs), 747

codecs, 493

commands

aaa authentication login default, 149

aaa new-model, 149

access-class, 486

access-list, 445, 457, 463-466, 486

any keyword, 448

building ACLs with, 454

deny keyword, 448-449

examples and logic explanations, 467

extended numbered ACL configuration commands, 467

log keyword, 452

permit keyword, 445, 448-449

reverse engineering from ACL to address range, 454-456

tcp keyword, 464

upd keyword, 464

authentication ppp pap, 346

auto-cost reference-bandwidth, 222, 643

auto-summary, 267, 270

EIGRP, 247

EIGRP for IPv4, 648

bandwidth, 216, 222, 270, 359

EIGRP, 247, 647

EIGRP for IPv6, 662

EIGRP metrics, 237, 265

OSPFv3 interface, 643

bgp, 311

channel-group (EtherChannels), 84, 95, 543

incorrect options, troubleshooting, 106-108

Layer 3, troubleshooting, 541

clear ip ospf process, 204, 223

clock rate, 349, 359

command, 222

configure terminal, 28

debug, 286

debug eigrp fsm, 271

debug eigrp packets, 286, 298

debug ip ospf adj, 298

mismatched OSPF areas, 290

OSPF neighbors, troubleshooting, 289

debug ip ospf events, 298

debug ip ospf hello, 298

Hello/dead timer mismatches, 293

OSPF neighbors, troubleshooting, 289

debug ip ospf packet, 298

debug ipv6 ospf adj, 632

debug ppp authentication, 356, 360

debug ppp negotiation, 360

debug spanning-tree events, 79, 96

default-information originate, 223, 321, 628

default-information originate always, 214

delay, 247, 270, 472-474

EIGRP, 647

EIGRP for IPv6, 662

EIGRP metrics, 237, 265

extended IPv6 ACLs, 675

IPv6 ACLs, 672

deny icmp any any, 683

description, 359

dialer pool, 417, 432

dns-server, 571

eigrp router-id, 246, 252

EIGRP, 647

EIGRP for IPv6, 662

encapsulation, 359, 525

encapsulation dot1q, 543

encapsulation ppp, 344, 350, 417, 432

erase startup-config, 135

frequency, 728

history buckets-kept 6, 728

history enhanced, 717

history enhanced interval, 728

history filter all, 728

history lives-kept 1, 728

hostname, 345

icmp-echo, 728

ifconfig, 568, 600, 615

interface, 25, 37, 543

interface dialer, 432

interface loopback, 196, 222

interface multilink, 360

interface multilink1, 350

interface port-channel, 543

interface range, 27

interface tunnel, 400, 432

interface vlan, 543

ip -6 neighbor show, 615

ip access-group, 450, 457, 467, 477, 486

ip access-list, 472, 486

ip access-list extended, 473

ip address, 568, 584-585

IP addresses on loopback interfaces, 196

MLPPP, 350

subinterfaces, 525

ip address negotiated, 418, 432

ip domain-lookup, 572

ip hello-interval eigrp, 247, 270, 297, 648

ip helper-address, 573-574

ip hold-time eigrp, 247, 270, 297

ip mtu, 296, 637

ip name-server, 572

ip ospf, 222

ip ospf cost, 222

ip ospf dead-interval, 297

ip ospf hello-interval, 297

ip route, 323

ip routing, 543

ip sla, 728

ip sla restart, 728

ip sla schedule, 715

ipconfig, 568, 600, 615

ipv6 access-list

building, 678-679

IPv6 ACLs, 687

ipv6 access-list deny, 678

ipv6 access-list permit, 678

ipv6 address, 598, 614

ipv6 dhcp relay destination, 614

ipv6 eigrp, 648, 662

ipv6 hello-interval eigrp, 662

ipv6 hold-time eigrp, 662

ipv6 mtu, 637

ipv6 ospf, 614, 624, 643

ipv6 ospf cost, 643

ipv6 router eigrp, 647, 662

ipv6 router ospf, 614, 624, 643

ipv6 traffic-filter, 673, 687

ipv6 unicast routing, 614

ipv6 unicast-routing, 598

mac-address, 432

maximum-paths, 218

defined, 222, 270

EIGRP, 247, 647

EIGRP for IPv6, 651, 662

EIGRP load balancing, 263

OSPFv3, 627, 643

monitor session, 721, 728

mtu, 432

name, 25, 40, 135

ndp -an, 615

neighbor, 322

neighbor shutdown, 314

netsh interface ipv6 show neighbors, 615

network

BGP, 323

BGP table entries, injecting, 314-320

EIGRP, 248, 270

EIGRP, enabling, 246

EIGRP for IPv4, 648

EIGRP for IPv6 compatibility, 647

OSPF single-area configuration, 198-200

OSPFv2 interface configuration, 218

OSPFv2 multiarea configuration, 209

no auto-summary, 268

no ip access-group, 476

no ip address, 539

no ip domain-lookup, 572

no ip sla schedule 1, 715

no neighbor shutdown, 314

no passive-interface, 223, 270

no shutdown, 40, 359

EIGRP for IPv6, 662

EIGRP for IPv6 routing, 650

Layer 1 leased-line WAN problems, 354

OSPF processes, 294

ROAS subinterfaces, 527

no spanning-tree portfast bpduguard default, 95

no spanning-tree portfast default, 95

no switchport

Layer 3 EtherChannels, 539

Layer 3 switches, 543

routed ports, 535

passive-interface, 205

defined, 222, 297

EIGRP, 270

EIGRP support, 251

OSPF interfaces as passive, configuring, 196

OSPFv3, 624

passive-interface default, 205, 270

permit, 471-474, 487

extended IPv6 ACLs, 675

GRE tunnel ACLs, 410

IPv6 ACLs, 672

permit gre, 432

permit icmp any any router-advertisement, 684

permit icmp any any router-solicitation, 684

permit ipv6, 687

ping, 483, 571-574, 615

IPv6 host connectivity, testing, 600

IPv6 routes, testing, 602, 614

leased-line WANs, 353

self-ping, 483-485

ping6, 615

IPv6 ACLs, 674

IPv6 connectivity, testing, 601

ppp authentication, 349, 359

ppp authentication chap, 345

ppp chap hostname, 432

ppp chap password, 432

ppp multilink, 350, 360

ppp multilink group, 360

ppp multilink group 1, 350

ppp pap sent-username, 346, 359

pppoe-client dial-pool-number, 417, 432

pppoe enable, 417, 432

remark, 472, 487

router bgp, 311

router eigrp, 246, 270, 647

router-id, 222, 614, 624

OSPFv3, 643

RIDs, defining, 196

router ospf, 196, 222

router ospf 1, 198

sdm prefer, 532

sdm prefer lanbase-routing, 543

show

IPv6 ACLs, 673

routing protocol-enabled interfaces, verifying, 275

STP status, 68

show access-list, 473

show access-lists, 450, 457, 479, 487, 687

show arp, 572

show controllers, 352

show controllers serial, 360

show etherchannel, 96, 543

show etherchannel 1 summary, 86

show etherchannel summary, 107, 540

show interfaces, 298, 360, 543, 569

EIGRP neighbor requirements, verifying, 286

MLPPP, 352

OSPF interfaces, troubleshooting, 283

OSPF neighbors, troubleshooting, 289

OSPFv3 interface bandwidth, 640

PPP CHAP status, 345

PPP PAP, 346

routed ports, 536

show interfaces description, 298, 576

show interfaces dialer, 421, 433

show interfaces PPP status, 344

show interfaces status

Layer 3 EtherChannels, 539

routed ports, 536

show interfaces switchport, 31-34, 37, 41, 114-116, 135 show interfaces trunk, 32-34, 38, 41, 116-117

show interfaces tunnel, 405, 433

show interfaces virtual-access, 433

show interfaces virtual-access configuration, 423

show interfaces vlan, 543

show ip access-list, 457, 474-476

show ip access-lists, 450, 479, 487

show ip bgp, 323

show ip bgp summary, 313, 323

show ip eigrp interfaces, 271, 297

EIGRP enabled interfaces, 250-251, 275

EIGRP neighbor requirements, verifying, 286

multilink interfaces, 352

show ip eigrp interfaces detail, 250, 271

show ip eigrp neighbors, 271, 297

neighbor status, displaying, 253

neighbor verification checks, 285

show ip eigrp topology, 259, 271

metrics, 262

successor routes, 258

topology table, 256

show ip eigrp topology all-links, 260

show ip interface, 450, 457, 479

show ip interface brief, 360

GRE tunnels, 404

multilink interfaces, 352

OSPF interfaces, troubleshooting, 283

show ip interfaces, 286

show ip ospf, 223, 298

duplicate OSPF RIDs, 291

OSPF neighbors, troubleshooting, 289

show ip ospf database, 179, 201, 223

show ip ospf interface, 223, 298

DRs/BDRs details, displaying, 211

Hello/dead timer mismatches, 293

OSPF areas for ABR interfaces, 210

OSPF neighbors, troubleshooting, 289

OSPFv2 interface configuration, 220

passive interface, 206

show ip ospf interface brief, 205, 223, 298

OSPF areas for ABR interfaces, 210

OSPF-enabled interfaces, identifying, 275

OSPF neighbors, troubleshooting, 289

OSPF status on interfaces, 281

OSPFv2 interface configuration, 221

show ip ospf neighbor, 182, 223, 298

DRs/BDRs details, displaying, 211

neighbors, listing, 288

OSPF processes shutdown, 295

show ip ospf neighbor interface brief, 295

show ip protocols, 223, 271, 297

EIGRP-enabled interfaces, 251-252, 275

EIGRP neighbor requirements, verifying, 286

EIGRP neighbor status, displaying, 253

IPv4 routing protocols, 202

OSPF configuration errors, 282-283

OSPFv2 interface configuration, 219

show ip route, 223, 271, 323, 577-580

administrative distance, 178

dialer interface Layer 3 orientation, 425

EIGRP-learned routes, displaying, 254

IPv4 routes added by OSPF, 201

routing tables, displaying, 543

show ip route eigrp, 254, 271, 297

show ip route ospf, 223, 298, 577-578

show ip route static, 214

show ip sla enhanced-history distribution-statistics, 729

show ip sla history, 717, 729

show ip sla statistics, 729

show ip sla summary, 729

show ipv6 access-list, 677, 687

show ipv6 eigrp interfaces, 654, 662

show ipv6 eigrp interfaces detail, 662

show ipv6 eigrp neighbors, 663

show ipv6 eigrp topology, 663

show ipv6 eigrp topology | section, 663

show ipv6 interface, 614, 687

show ipv6 neighbors, 614

IPv6 ACL ICMPv6 NDP message filtering, 681

IPv6 IPv4 replacement, 603

show ipv6 ospf, 640, 643

show ipv6 ospf database, 636, 643

show ipv6 ospf interface, 630-631, 643

show ipv6 ospf interface brief, 630, 640, 643

show ipv6 ospf neighbor, 635, 643

show ipv6 protocols, 614, 643

EIGRP for IPv6, 662

EIGRP for IPv6 interfaces, 654

OSPFv3 interfaces, 630

show ipv6 route, 614, 643

EIGRP for IPv6, 663

IPv6 router connectivity, 603

show ipv6 route eigrp, 663

show ipv6 route ospf, 638, 643

show ipv6 route | section, 663

show ipv6 routers, 614, 681

show mac address-table, 114

show mac address-table dynamic, 111

show monitor detail, 724, 729

show monitor session, 724, 729

show monitor session all, 723

show ppp all, 346-347, 360

show ppp multilink, 353, 360

show pppoe session, 424, 433

show running-config, 135, 449, 473-475

show snmp, 703, 729

show snmp community, 702, 728

show snmp contact, 728

show snmp group, 709, 729

show snmp host, 702, 729

show snmp location, 728

show snmp user, 708, 729

show spanning-tree, 96

show spanning-tree bridge, 81

show spanning-tree interface, 96

show spanning-tree interface detail, 82

show spanning-tree root, 77, 81

show spanning-tree summary, 83, 96

show spanning-tree vlan, 96

show spanning-tree vlan 10, 75-77

show spanning-tree vlan 10 bridge, 77

show spanning-tree vlan 10 interface gigabitethernet0/2 state, 92

show standby, 556, 560, 565

show standby brief, 555, 565

show tcp brief, 313

show tcp summary, 323

show vlan, 41, 114, 141

show vlan brief, 26-29, 114

show vlan id, 27, 114

show vlan status, 135

show vlans, 527, 543

show vtp password, 134, 141

show vtp status, 29, 41, 131, 134, 141

shutdown, 40, 359

EIGRP for IPv6, 662

EIGRP for IPv6 routing, 650

Layer 1 leased-line WAN problems, 354

OSPF processes, 294

ROAS subinterfaces, 527

shutdown vlan, 135, 140

snmp-server, 700

snmp-server community, 727

snmp-server contact, 727

snmp-server enable traps, 727

snmp-server group, 705

snmp-server host, 701, 710, 727

snmp-server location, 727

snmp-server user, 707

spanning-tree, 95

spanning-tree bpduguard disable, 95

spanning-tree bpduguard enable, 75, 81, 95

spanning-tree mode, 88, 95

spanning-tree mode mst, 72

spanning-tree mode pvst, 72

spanning-tree mode rapid-pvst, 72, 90

spanning-tree pathcost method long, 55

spanning-tree portfast, 75, 81, 95

spanning-tree portfast bpduguard, 95

spanning-tree portfast default, 83, 95

spanning-tree portfast disable, 83, 95

spanning-tree vlan, 74

spanning-tree vlan 10 port-priority 112, 103

speed, 576

standby, 554, 564

standby 1 preempt, 558

standby version, 559

standby version 1 | 2, 564

switchport

Layer 3 switches, 543

routed ports, 535

switchport access vlan, 25, 28-29, 37-38, 40, 113, 135

switchport mode, 30, 40

switchport mode access, 25, 28, 37-38, 139

switchport mode dynamic auto, 116

switchport mode dynamic desirable, 32

switchport mode trunk, 30, 116, 524

switchport nonegotiate, 34, 40, 116, 139

switchport trunk allowed vlan, 41, 117

switchport trunk encapsulation, 30, 40

switchport trunk native vlan, 40, 118

switchport voice vlan, 36-38, 41, 135

traceroute, 574

GRE tunnels, 406

IPv6 host connectivity, testing, 600

IPv6 network router problems, troubleshooting, 611
IPv6 router connectivity, testing, 602, 614
traceroute6, 615
tracert, 615
tunnel destination, 406-408, 432
tunnel mode gre ip, 404, 432
tunnel mode gre multipoint, 404
tunnel source, 406-407, 432
undebug all, 298
username, 345, 359
variance, 270
EIGRP, 247, 263, 647
EIGRP for IPv6, 651, 662
verification, 75
vlan, 25, 37, 40, 135
vlan 10, 122
vlan 200, 137
vtp, 134
vtp domain, 134, 140
vtp mode, 40, 134, 140
vtp mode off, 29, 135
vtp mode transparent, 29, 135
vtp password, 134, 140
vtp pruning, 134, 140
vtp version, 140
committed information rate (CIR), 373, 509
communities (SNMP), 698-699
Community-based SNMP Version 2 (SNMPv2c), 699
community strings (SNMP), 698
confidentiality (Internet VPNs), 393
Config Checklist app, 796
configure terminal command, 28
configuring
AAA servers, 148-150
AAA servers for 802.1x, 145
ACLs (access control lists)
extended numbered, 467-470
named, 472
numbered, 475-476
standard numbered, 448-452
BGP, 310
disabling eBGP neighbors, 314
eBGP neighbor verification, 312-313
eBGP neighbors using link addresses, 311-312
ISP default routes, learning, 320-321
table entries, injecting, 314-320
transporting messages with TCP, 310
update messages, 310
BPDU Guard, 81-83
DHCP snooping, 153-154
EIGRP, 246
ASNs, 248
checklist, 246
classful network numbers, 248
classic versus named mode, 249
sample internetwork, 247
verification. See *verifying, EIGRP configuration*
wildcard masks, 248-249
EIGRP for IPv6, 647
commands, 647
example, 648-649
load balancing, 651-652
route metrics, 650-651
timers, 652

EtherChannels, 84
- *dynamic, 86-87*
- *manual, 84-86*

GRE tunnels, 402-404

HDLC, 337-340

HSRP, 554, 560-561

ICMP-Echo operations, 714-715

IGPs, 310

interfaces as passive, 205

IPv6
- *addressing on routers, 598-599*
- *extended ACLs, 674-676*
- *hosts, 595-597*
- *routing, 598*
- *standard ACLs, 671-674*
- *static routes, 599*

ISL, 525

ISP routers, 419

Layer 3
- *EtherChannels, 537-539*
- *switch routed ports, 535-537*
- *switching with SVIs, 529-531*

local SPAN, 721-724

MLPPP, 349-350

multiarea OSPFv2, 206-210
- *network commands, 209*
- *single-area configurations, 207-208*
- *subnets, 206*
- *verifying, 210-212*

OSPFv2 interfaces, 218-221

OSPFv3, 621
- *default routes, 627-628*
- *load balancing, 627*
- *multiarea example, 622*
- *multiarea on ABR, 625*
- *route selection metrics, setting, 626*
- *single-area, 623-624*

overlapping VLSM subnets, 584-585

PortFast, 81-83

PPP, 343-344
- *CHAP, 344-345*
- *PAP, 346-347*

PPPoE, 415-416
- *ISP router configuration example, 419*
- *Layer 1, 416-417*
- *Layer 2, 417-418*
- *summary, 418-419*
- *verification, 420-425*

RIDs (OSPF), 203-204

ROAS, 524
- *native VLANs, 525-526*
- *subinterface numbers, 525*
- *subinterfaces, creating, 524-525*
- *troubleshooting, 528-529*
- *verifying, 526-527*

single-area OSPFv2, 197-198
- *IPv4 addresses, 197*
- *matching with network command, 198-200*
- *multiarea configurations, 207-208*
- *network command, 198*
- *organization, 196-197*
- *passive interfaces, 204-206*
- *RIDs, 203-204*
- *verifying, 200-202*
- *wildcard masks, 199*

SNMPv2
- *Get/Set messages, 699-701*
- *Trap/Inform messages, 701-702*
- *verifying, 702-704*

SNMPv3, 704
authentication, 707-708
encryption, 707-708
groups, 705-707
notifications, 710-711
requirements, 704
summary, 711-712
users, 707
verifying, 708-709
STP, 71
modes, 72
options, 74-75
per-VLAN port costs, 74
port costs, 78-79
PVST+, 72-73
root election influence, 80-81
system ID extensions, 73-74
topology changes, influencing, 55
verification commands, 75
VLANs (virtual LANs), 24-25
data and voice VLANs, 36-38
full VLAN configuration example, 25-28
shorter VLAN configuration example, 28-29
trunking, 30-34
VTP
common rejections, troubleshooting, 137
default VTP settings, 129
example, 130-131
new VTP configuration settings, 130
planning, 129
steps, 129
storing configuration, 134-135
transparent mode, 135

congestion avoidance, 512
TCP windowing, 512-513
tools, 513-514
congestion management, 504
Low Latency Queuing (LLQ), 505-507
multiple queues, 504
output queuing, 504
prioritization, 505
round robin scheduling, 505
strategy, 507
connections (public cloud access)
branch offices, 751
Internet, 745-746
private WANs, 746-749
VPNs, 747
contiguous networks, 267
control planes
centralized, 766
distributed, 766
networking devices, 763-764
control protocols (CP), 341
controllers, 766
APIC-EM, 777
centralized control, 766-767
Northbound Interfaces (NBIs), 768-770
OpenDaylight SDN controller, 771
Southbound Interfaces (SBIs), 767-768
convergence
EIGRP, 239
DUAL process, 242-243
feasible successor routes, 260-261
successors, 241-242
routing protocols, 173
STP, 48, 105-106

converting

binary to hexadecimal, 808

decimal to binary, 805-807

hexadecimal to binary, 808

core switches, 159-160

CoS (Class of Service) fields (802.1Q header), 500-501

costs. ***See*** **metrics**

counters, 715-716

CP (control protocols), 341

CPE (customer premises equipment), 332

CS (Class Selector), 503

CS DSCP values, marking, 503

CSRs (Cloud Services Routers), 747

CSU/DSU (channel service unit/data service unit), 332-334

CUCM (Cisco Unified Communication Manager), 35

customer edge (CE), 377

D

data

application traffic, 492-493

EIGRP for IPv6 topology, 657-658

integrity, 393

usage (MetroE), 373

bandwidth used, charging for, 373-374

overages, controlling, 374-375

data centers (virtual)

networking, 735

physical networks, 736

vendors, 735

workflow, 737-738

data circuit-terminating equipment (DCE), 334

data plane

EtherChannel impact on MAC tables, 111-112

networking devices, 762-763

STP impact on MAC tables, 110

VLAN of incoming frames, 112-113

data terminal equipment (DTE), 334-335

databases

LSDB, 179

area design, 190

best routes, finding, 180

contents, displaying, 201

exchanging between neighbors, 183-186

LSAs relationship, 179

OSPFv3, 636

MIB, 695-697

OIDs, 697

variable numbering/names, 697

variables, monitoring, 696

views, 705

topology, 188

VLAN, 131-133

DCE (data circuit-terminating equipment), 334

Dead Interval timer, 184

dead timers, 293-294

debug command, 286

debug eigrp fsm command, 271

debug eigrp packets command, 286, 298

debug ip ospf adj command, 298

mismatched OSPF areas, 290

OSPF neighbors, troubleshooting, 289

debug ip ospf events command, 298

debug ip ospf hello command, 298
Hello/dead timer mismatches, 293
OSPF neighbors, troubleshooting, 289
debug ip ospf packet command, 298
debug ipv6 ospf adj command, 632
debug messages, 261
debug ppp authentication command, 356, 360
debug ppp negotiation command, 360
debug spanning-tree events command, 79, 96
decimal-to-binary conversion, 805-807
decimal wildcard masks, 446-447
default-information originate always command, 214
default-information originate command, 223, 321
OSPF default routes, 214
OSPFv3, 628
default routes, 627-628
default VLANs, 25
delay command, 270
EIGRP, 247, 647
EIGRP for IPv6, 662
EIGRP metrics, 237, 265
delays
EIGRP
IPv6 routes, 650-651
metrics, 237, 265
managing, 491
delivery headers, 400
deny command, 472-474, 487
extended IPv6 ACLs, 675
IPv6 ACLs, 672
deny icmp any any command, 683
deny keyword, 442, 448-449
dependencies (SPAN), 722
description command, 359
design
improving with chassis aggregation, 160
Internet edge, 306
MetroE Layer 3, 370
E-LAN service, 371-372
E-Line service, 370-371
E-Tree service, 372
MetroE physical, 365-366
MPLS Layer 3, 377
MPLS VPNs Layer 3, 379-382
OSPF area, 189
ABR, 190, 210-211
areas, 189-190
backbone areas, 190
backbone routers, 190
benefits, 191
interarea routes, 190
internal routers, 190
intra-area routes, 190
MPLS VPNs, 381-382
network size, 189
problems, 188, 281
single-area, 188
SPF workload, reducing, 190
three-area, 189
OSPFv3 multiarea, 622
designated ports. ***See*** **DPs**
designated routers. ***See*** **DRs**
destination addresses, 406
destination IP, matching, 463-464
destination ports (SPAN), 719
devices, networking, 762
control, centralizing, 766-767
control plane, 763-764

data plane, 762-763

management plane, 764

switch internal processing, 765-766

DevNet, 777

DHCP (Dynamic Host Control Protocol)

Binding Table, 153

DHCP Relay, 573

public cloud services, 757

snooping

configuration settings, 153

DHCP-based attacks, 152

DHCP Binding Table, 153

features, 151

ports as trusted, configuring, 153

rate limiting, 154

rules summary, 153

trusted/untrusted ports, 151-154

stateful, 608-609

troubleshooting, 573-574

DHCP-based attacks, 152

DHCPv6, 596

dialer interfaces

Layer 3 orientation, 425

PPPoE

configuration, 416-417

verifying, 421-422

dialer pool command, 417, 432

Differentiated Services Code Point. ***See*** **DSCP**

Diffusing Update Algorithm (DUAL), 242-243, 646

Digital Signal level 0 (DS0), 334

Digital Signal level 1 (DS1), 334

Digital Signal level 3 (DS3), 334

digital subscriber lines (DSLs), 390-391

Dijkstra SPF algorithm, 180

direction (ACLs), 440-441

disabling

BGP neighbors, 314

BPDU Guard, 83

DTP, 116

EIGRP for IPv6 routing, 650

PortFast, 83

ports, 60

VLANs, 114-115

VLAN trunking, 139

discard routes, 319

discarding state

interfaces, 47-49

RSTP, 61

discontiguous classful networks, 266-268

discontiguous networks, 267

discovery (EIGRP neighbors), 234

displaying

BPDU Guard global settings, 83

DRs/BDRs details, 211

EIGRP

enabled interfaces, 275

IPv4 routing table, 253-254

neighbor status, 253

topology table, 255-257

LSDB contents, 201

OSPF-enabled interfaces, 275

passive interfaces, 206

PortFast global settings, 83

TCP connections, 313

distance vector protocols. ***See*** **DV protocols**

distributed control planes, 766

distribution switches, chassis aggregation, 159-160

DMVPN (Dynamic Multipoint VPN), 411

multipoint GRE tunnels, 411

NHRP (Next Hop Resolution Protocol), 412-413

DNS (Domain Name System)

IPv6 network troubleshooting, 607-608

public cloud services, 754-756

troubleshooting, 571-572

dns-server command, 571

down status (interfaces), 354

DP (designated port), LAN segments, 49, 60

choosing, 54, 104-105

problems, troubleshooting, 105

DR (designated router), 185

backup (BDRs), 185

discovering, 211-212

Ethernet links, 185-186

DROthers routers, 186

DS0 (Digital Signal level 0), 334

DS1 (Digital Signal level 1), 334

DS3 (Digital Signal level 3), 334

DSCP (Differentiated Services Code Point), 497

fields (QoS marking), 501

marking values

AF, 502-503

CS, 503

EF, 502

DSL (digital subscriber line), 390-391

DSLAMs (DSL access multiplexers), 390

DTE (data terminal equipment), 334-335

DTP (Dynamic Trunking Protocol), 116

DUAL (Diffusing Update Algorithm), 242-243, 646

dual Internet edge design, 306

dual stack

OSPFv2/OSPFv3, 619

OSPFv3 address families, 620

strategies, 598

DV (distance vector) protocols, 175, 228

distance/vector information learned, 228

EIGRP as, 232-233

route poisoning, 231-232

split horizon, 230-231

update messages, 229-230

dynamic EtherChannels configuration, 86-87

Dynamic Host Control Protocol. *See* DHCP

Dynamic Multipoint VPN. *See* DMVPN

Dynamic Trunking Protocol (DTP), 116

E

E1, 334

E3, 334

EAP (Extensible Authentication Protocol), 146

EAPoL (EAP over LAN), 146

earplugs (exam), 786

eBGP (External BGP), 304

Internet edge, 306

design, 306

enterprise public prefixes, advertising, 307-308

ISP default routes, learning, 309

neighbors
configuring, 312
disabling, 314
using link addresses, configuring, 311
verifying, 312-313

Eclipse IDE, 744

edge ports, 63

EF (Expedited Forwarding), 501

EF DSCP value marking, 502

EF RFC (RFC 3246), 502

EGP (exterior gateway protocol), 173, 302

EIGRP (Enhanced Interior Gateway Routing Protocol), 175

EIGRP for IPv4

as advanced DV protocol, 232-233
authentication, 286
autosummarization, 266
classful network boundaries, 266-267
discontiguous classful networks, 267-268
benefits, 227
configuration, 246
ASNs, 248
checklist, 246
classful network numbers, 248
classic versus named mode, 249
sample internetwork, 247
wildcard masks, 248-249
convergence, 239
DUAL process, 242-243
feasible successor routes, 260-261
successors, 241-242
disadvantages, 227
EIGRP for IPv6, compared, 644-646, 653
feasible successor routes
convergence, 260-261
identifying, 258-260
goals, 302
interfaces
configuration problems, 278-281
identifying, 275
OSPF interfaces, compared, 281
troubleshooting, 275-281
K-values, 286
metrics, 236
bandwidth, 265
calculation, 236-237
components, 262
delay settings, 265
EIGRP topology database, 262
example, 237-238
FD (feasible distance), 240-241
RD (reported distance), 240-241
route load balancing, 264
serial link bandwidth, 238-239
MPLS VPN challenges, 382
neighbors, 234-235
discovery, 234
requirements, 284-286
status, 233, 253
topology information, exchanging, 235-236
troubleshooting example, 286-288
verifying, 235, 285-286
OSPF, compared, 224
query/reply messages, 242
RIDs, configuring, 252
RIP metrics, compared, 176

RIPv2/OSPFv2, compared, 233

routes

choosing, 234

load balancing, 263-264

tuning with bandwidth changes, 259

variance, 263-264

successor routes, identifying, 257-258

topology

database metrics, 262

exchange, 234

table, displaying, 255-257

variance, 263-264

verification, 249

EIGRP enabled interfaces, finding, 250-252

IPv4 routing table, displaying, 253-254

neighbor status, displaying, 253

EIGRP for IPv6

configuration, 647

commands, 647

example, 648-649

load balancing, 651-652

route metrics, 650-651

timers, 652

DUAL, 646

EIGRP for IPv4, compared, 644-646, 653

FS, 646

interfaces, 654-655

neighbors, 656-657

routes

ASNs, 649

enabling/disabling, 650

FS, 646

successors, 646

troubleshooting, 660

verifying, 659-660

topology data, 657-658

eigrp router-id command, 246, 252, 647, 662

E-LAN (Ethernet LAN) service, 368-372

E-Line (Ethernet Line) service, 367-371

email, 750-751

enabling

AAA servers, 149

BPDU Guard, 83

EIGRP, 246

EIGRP for IPv6 routing, 650

IPv6 routing, 598

OSPF configuration mode, 198

PortFast, 83

PPPoE, 417

VLANs, 115

Encapsulated RSPAN (ERSPAN), 721

encapsulation command, 359, 525

encapsulation dot1q command, 543

encapsulation ppp command, 344, 350, 417, 432

encryption

IPsec, 395-396

keys, 395

SNMPv3, 699, 707-708

tunnel VPNs, 395

***End-to-End QoS Network Design*, Second Edition (Cisco Press), 494**

end-user traffic, measuring, 713

endpoints, 773

enhanced history, 717

Enhanced Interior Gateway Routing Protocol (EIGRP), 175. *See also* EIGRP for IPv4; EIGRP for IPv6

Enterprise QoS Solution Reference Network Design Guide, 494

enterprises, classification matching, 496-497

eq 21 parameters, 465

erase startup-config command, 135

ERSPAN (Encapsulated RSPAN), 721

EtherChannels, 64-65

- configuring, 84
  - *dynamic, 86-87*
  - *manual, 84-86*
- Layer 3
  - *configuring, 537-539*
  - *troubleshooting, 541*
  - *verifying, 539-540*
- MAC tables impact, predicting, 111-112
- troubleshooting, 106
  - *configuration checks before adding interfaces, 108-109*
  - *incorrect options, 106-108*

Ethernet

- 802.1Q headers, 500-501
- 802.11 headers, 501
- access links, 365
- carrier, 366
- IEEE standards, 366
- links, 185-186
- WANs, 747

Ethernet LANs

- service, 368-372
- troubleshooting, 575-576
- VLANs (virtual LANs)
  - *configuration, 24-29*
  - *default VLANs, 25*
  - *IDs, 18*
  - *IP telephony, 34-39*
  - *native VLANs, 20*
  - *overview, 16-18*
  - *routing between, 21-24*
  - *tagging, 18-20*
  - *trunking, 18-21, 29-34*

Ethernet Line (E-Line) service, 367-371

E-Tree (Ethernet Tree) service, 369, 372

ETSI (European Telco standards body), 754

EUI-64 rules, 597-599

EVC (Ethernet Virtual Connection), 367

exact IP address matching, 445-446

exam

- CLI skills, 794-796
- earplugs, 786
- exam-day suggestions, 787
- knowledge gaps, finding, 792-793
- practice exams
  - *answering questions, 790-791*
  - *CCNA R&S, 790*
  - *checklist, 790*
  - *ICND2, 790*
  - *other, 792*
  - *taking, 789-790*
- pre-exam suggestions, 786-787
- preparing for failure, 788
- question types, 784
- ready to pass assessment, 797
- scores, 796-797
- study tasks, 798
- studying after failing to pass, 797-798
- time budget versus number of questions, 785
- time-check method, 786
- tutorial, 784-785

Expedited Forwarding (EF), 501

extended IPv6 ACLs

configuring, 674-676

examples, 676-678

extended numbered IPv4 ACLs, 462

configuration, 467-470

matching protocol, source IP, and destination IP, 463-464

matching TCP and UDP port numbers, 464-467

Extensible Authentication Protocol (EAP), 146

exterior gateway protocol (EGP), 173, 302

external BGP. ***See*** **eBGP**

F

Facebook (Wendell Odom), 799

failed interfaces, 49

failing the exam, 788, 797-798

failures

CHAP authentication, 356

HSRP, 552

keepalive, 355

PAP authentication, 356

FCS (Frame Check Sequence), 336

FD (feasible distance), 240-241, 256

feasibility conditions, 242, 260

feasible successor (FS), 646

feasible successor routes, 241-242

convergence, 260-261

identifying, 258-260

FHRP (First Hop Redundancy Protocol), 544

features, 550

HSRP, 551

active/passive model, 551

active/standby routers, choosing, 555

active/standby rules, 557

configuring, 554

failover, 552

group numbers, 555

load balancing, 553

no preemption, 557

with preemption, 558

troubleshooting, 560-563

verifying, 555-556

versions, 559-560

need for, 549

options, 550-551

fiber Internet, 393

FIFO (first-in, first-out), 504

filtering

ICMPv6 messages, 668-669, 679-683

IPv6

ACL policies, 668

issues, 604

finding

EIGRP

enabled interfaces, 250-252

feasible successor routes, 258-260

successor routes, 257-258

mismatched Hello/dead timers, 293

OSPF area mismatches, 290-291

routers best routes, 180

wildcard masks, 448

firewalls, 754

First Hop Redundancy Protocol. ***See*** **FHRP**

first-in, first-out (FIFO), 504
FlexStack, 158
FlexStack-Plus, 158
flooding, 179
flow
networking, 493
public cloud traffic, 750-751
Forward delay timer (STP), 56
forwarding
data. *See* routing
interface state, 47-49
paths, 777-778
forwarding plane. *See* data plane
Fractional T1, 334
Fractional T3, 334
Frame Check Sequence (FCS), 336
Frame Relay, 362
frames
broadcast storms, 45-47
defined, 495
HDLC, 336
incoming, 112-113
looping, preventing, 44
multiple frame transmissions, 47
PPP, 341
switching, 113
frequency command, 728
FS (feasible successor), 646
full drops, 514
full mesh topology (MetroE), 368
full neighbor state, 186, 628
full updates, 229, 235
full VLAN configuration example, 25-28
fully adjacent neighbors, 186, 633

G

generic routing encapsulation (GRE), 398
"Get IEEE 802" program, 59
Get messages
agent information, 696
RO/RW communities, 699
SNMPv2 support, 699-701
GLBP (Gateway Load Balancing Protocol), 544
global unicast addresses, 593
Google App Engine PaaS, 744
GRE (generic routing encapsulation), 398
GRE tunnels, 398
between routers, 399
configuring, 402-404
details, displaying, 404
functionality, testing, 406
large scale environments, 411
multipoint with DMVPN, 411
point-to-point, 399
routes, 405
troubleshooting, 406
ACLs, 409-410
interface state, 407
Layer 3 issues, 409
source/destination addresses, 406
tunnel destination, 408
tunnel interfaces, 398
unsecured networks, 400-401
verifying, 404-406
group numbers (HSRP), 555

groups
- endpoint, 773
- SNMPv3, 705-707
  - *MIB views, 705*
  - *security levels, 705*
  - *write views, 706*

H

HDLC (High-level Data Link Control), 331, 336-340, 398

headers
- 802.1Q, 500-501
- 802.11, 501
- delivery, 400
- IP, 499-501
- MPLS Label, 501

Hello BPDU, 49

Hello Interval, 184, 233

Hello messages (OSPF), 181-182

Hello timer
- dead timer mismatches, troubleshooting, 293-294
- STP, 56

hexadecimal-to-binary conversion, 808

high availability, 159-160

High-level Data Link Control (HDLC), 331, 336-340, 398

High-speed WICs (HWICs), 332

historical success/failure counters (IP SLAs), 716

history
- IP SLA data, 717
- OSPF, 619
- SNMP, 695

history buckets-kept 6 command, 728

history enhanced command, 717

history enhanced interval command, 728

history filter all command, 728

history lives-kept 1 command, 728

Hold Interval, 233

hostname command, 345

hosts
- IPv6, 595
  - *connectivity, verifying, 600-601*
  - *issues, 604*
  - *missing settings, 608-610*
  - *name resolution problems, 607-608*
  - *pings fail from default router, 606-607*
  - *pings only working in some cases, 605-606*
  - *stateful DHCPv6, 596*
  - *stateless address autoconfiguration (SLAAC), 597*
- routes, 357
- server virtualization, 734
- troubleshooting IPv4 settings
  - *default router IP address setting, 572*
  - *DNS problems, 571-572*
  - *ensuring IPv4 settings match, 568-569*
  - *mismatched masks, 569-571*

HSRP (Hot Standby Router Protocol), 544, 551
- active/passive model, 551
- active/standby routers, choosing, 555
- active/standby rules, 557
- configuring, 554
- failover, 552
- group numbers, 555

load balancing, 553
no preemption, 557
with preemption, 558
troubleshooting, 560
ACL blocks HSRP packets, 563
configuration, 560-561
group number mismatches, 563
misconfiguration symptoms, 561
routers configuring different VIPs, 563
version mismatches, 562
verifying, 555-556
versions, 559-560
HSRPv2 (HSRP version 2), 559
hub and spoke topology (MetroE), 369
Huston, Geoff website, 303
HWICs (High-speed WICs), 332
hypervisors, 734

I

IaaS (Infrastructure as a Service), 742
IANA (Internet Assigned Numbers Authority), 174
ASNs, assigning, 174
ICMPv6 parameters, 669
IPv6 multicast address space registry website, 682
website, 174
iBGP (Internal BGP), 304
icmp-echo command, 728
ICMP-Echo operations, 714-715
ICMP Echo probe, 713
icmp keyword, 481
ICMPv6
Echo Request messages, 674
messages, filtering, 668-684
packets, matching, 675
ICND2 practice exam. *See* practice exams
IEEE (Institute of Electrical and Electronics Engineers)
802.1D Spanning-Tree states, 58
802.1D standard, 58
802.1w amendment, 58
802.1x
access, securing, 144-145
authenticators, 145
LAN access, securing, 145-146
default port costs, 55
Ethernet standards, 366
"Get IEEE 802" program, 59
ifconfig command, 568, 600, 615
IGP (interior gateway protocol), 173, 226
BGPs, compared, 302
classless/classful, 177
configuring, 310
goals, 302
metrics, 175-176
routing protocol algorithm, 175
subnets, 303
IGRP (Interior Gateway Routing Protocol), 175
implicit filtering, 683-684
incoming frames, 112-113
inferior Hello, 50
infinity, 231
Inform messages, 696-697
SNMPv2, 701-702
SNMPv3, 710-711
Infrastructure as a Service (IaaS), 742
injecting BGP table entries, 314
advertising subnets to ISPs, 318
classful network routes, 315-318
static discard routes, 319-320

instantiating VMs, 742

Institute of Electrical and Electronics Engineers. *See* IEEE

Integrated Intermediate System to Intermediate System (IS-IS), 175

interactive data application traffic, 492

interactive voice traffic, 494

interarea routes, 190, 212, 640

intercloud exchanges, 748-749

Intercloud Fabric, 749

interface command, 25, 37, 543

interface dialer command, 432

interface loopback command, 196, 222

interface multilink command, 360

interface multilink 1 command, 350

interface port-channel command, 543

interface range command, 27

interface tunnel command, 400, 432

interface vlan command, 543

interfaces

- ABR OSPF areas, verifying, 210-211
- access, 113-114
- administratively shutdown, 49
- application programming (APIs), 768-769
- bandwidth
  - *defaults, 216*
  - *EIGRP metric calculations, 265*
  - *EIGRP routes, tuning, 259*
  - *higher reference, 217*
  - *OSPF costs based on, 216-217*
- blocking state, 47
- delays, 265
- dialer
  - *Layer 3 orientation, 425*
  - *PPPoE, 416-417, 421-422*
- down status, 354
- EIGRP
  - *configuration problems, 278-281*
  - *enabled, finding, 250-252, 275*
  - *OSPF interfaces, compared, 281*
  - *troubleshooting, 275-281*
- EIGRP for IPv6, 654-655
- EtherChannels, adding, 108-109
- failed, 49
- forwarding state, 47
- LAN speeds, 490
- learning state, 58
- listening state, 58
- loopback, 203
- multilink, 349
- Northbound (NBIs), 768-770
- OSPF
  - *bandwidth, 216*
  - *costs, setting, 216-217*
  - *EIGRP interfaces, compared, 281*
  - *identifying, 275*
  - *passive, 196*
  - *troubleshooting, 281-283*
- OSPFv2 configuration, 218
  - *example, 218*
  - *verifying, 219-221*
- OSPFv3, 630
  - *influence route selections, setting, 626*
  - *troubleshooting, 631-632*
  - *verifying, 630-631, 638-640*
- passive
  - *EIGRP, 251*
  - *OSPF, 204-206*
  - *OSFPv3, 624*
- per-VLAN STP costs, 74

routed, 535-537

routing protocol-enabled, verifying, 274

Southbound (SBIs), 767-768

states

changing with STP, 57-58

forwarding or blocking criteria, 48-49

status codes, 353

subinterfaces, 524-527

switched virtual. *See* SVIs

tunnel

ACLs, 409-410

creating, 400

destinations, 408

Layer 3 issues, 409

replacing serial links, 398

state, 407

virtual-access, 423

VLAN. *See* SVIs

WANs, 490

working, 49

interior gateway protocol. *See* IGP

Interior Gateway Routing Protocol (IGRP), 175

interior IP routing protocols, 233

internal BGP (iBGP), 304

internal processing (switches), 765-766

internal routers, 190, 623-624

Internet

access, 389

cable Internet, 391

DSLs (digital subscriber lines), 390-391

fiber, 393

WANs, 389

wireless WANs, 392-393

edge, eBGP and, 306

design, 306

enterprise public prefixes, advertising, 307-308

ISP default routes, learning, 309

public cloud

accessing, 745-746

computing branch office connections, 751

VPNs, 389

benefits, 394

clients, 396-397

security, 393

site-to-site, 395-396

as WAN service, 389

wireless, 393

Internet Assigned Numbers Authority. *See* IANA

Internet service providers. *See* ISPs

Inter-Switch Link (ISL), 20-21, 525

intra-area routes, 190

ip -6 neighbor show command, 615

ip access-group command, 450, 457, 467, 477, 486

ip access-list command, 472, 486

ip access-list extended command, 473

IP ACLs (access control lists). *See* ACLs

ip address command, 568, 584-585

IP addresses on loopback interfaces, 196

MLPPP, 350

subinterfaces, 525

ip address negotiated command, 418, 432

ip_address parameter (network command), 198

IP addressing
  conversions
    binary-to-hexadecimal, 808
    decimal-to-binary, 805-807
    hexadecimal-to-binary, 808
  public clouds
    address assignment services, 756-757
    DHCP services, 757
ip domain-lookup command, 572
IP headers, 499-501
ip hello-interval eigrp command, 247, 270, 297, 648
ip helper-address command, 573-574
ip hold-time eigrp command, 247, 270, 297
IP IGP metrics, 175-176
ip mtu command, 296, 637
ip name-server command, 572
ip ospf command, 222
ip ospf cost command, 222
ip ospf dead-interval command, 297
ip ospf hello-interval command, 297
ip route command, 323
ip routing command, 543
ip sla command, 728
ip sla restart command, 728
IP SLAs (IP Service Level Agreements), 712
  historical success/failure counters, 716
  history data, troubleshooting with, 717
  ICMP-Echo, 713-715
  operations, 713
  responders, 713
  sources, 713
  troubleshooting with
    counters, 715-716
    history data, 717
  UDP Jitter probes, 713
ip sla schedule command, 715
IP telephony (VLANs), 34
  data and voice VLAN concepts, 34-36
  data and voice VLAN configuration and verification, 36-38
  summary, 38-39
ipconfig command, 568, 600, 615
IPP (IP Precedence) fields (QoS marking), 501-503
IPsec, 395-396
IPv4 routing
  ACLs, 666-667
  addresses, 197, 619
  EIGRP
    configuration, 248-249
    load balancing, 263-264
    verifying, 253-254
  EIGRP verification, 249
    EIGRP enabled interfaces, finding, 250-252
    IPv4 routing table, displaying, 253-254
    neighbor status, displaying, 253
  Layer 3 EtherChannels
    configuring, 537-539
    troubleshooting, 541
    verifying, 539-540
  Layer 3 switch routed ports, 534-537
  Layer 3 switching with SVIs
    configuring, 529-531
    troubleshooting, 532-534
    verifying, 531

matching addresses

any/all addresses, 448

exact IP address, 445-446

subset of address, 446-447

OSPF added, 201

QoS marking, 499

routing protocols

displaying, 202

troubleshooting, 273-274

subnet masks

mismatched masks, 569-571

VLSM (variable length subnet masking), 581

troubleshooting, 572

default router IP address setting, 572

DHCP issues, 573-574

DNS problems, 571-572

incorrect addressing plans, 581-585

IP forwarding issues, 577-580

LAN issues, 575-576

mismatched IPv4 settings, 568-569

mismatched masks, 569-571

packet filtering with access lists, 586

router WAN interface status, 585

ipv6 access-list commands

building, 678-679

IPv6 ACLs, 687

ipv6 access-list deny command, 678

ipv6 access-list permit command, 678

ipv6 address command, 598, 614

ipv6 dhcp relay destination command, 614

ipv6 eigrp command, 648, 662

ipv6 hello-interval eigrp command, 662

ipv6 hold-time eigrp command, 662

ipv6 mtu command, 637

ipv6 ospf command, 614, 624, 643

ipv6 ospf cost command, 643

ipv6 router eigrp command, 647, 662

ipv6 router ospf command, 614, 624, 643

IPv6 routing

access restrictions with IPv6 ACLs, 685

ACLs, 664-666

access-list commands, building, 678-679

access restrictions, 685

blocking, 683

capabilities, 669

extended, 674-678

filtering ICMPv6 NDP messages, 679-683

filtering policies, 668

ICMPv6 message filtering, 668-669

implicit filtering ICMPv6 NDP messages, 683-684

IPv4 ACL, compared, 666-667

limitations, 669-670

logging, 670

management control, 685

prefix lengths, 670

problems, 612

router originated packets, 670

standard, configuring, 671-674

testing, 677

tunneled traffic matching, 670

addressing on routers configuration, 598-599

connectivity, verifying, 600-601

hosts, 600-601

routers, 601-603

EIGRP
ASNs, 649
configuration, 647-649
DUAL, 646
EIGRP for IPv4, compared, 644-646, 653
FS, 646
interfaces, 654-655
load balancing, 651-652
neighbors, 656-657
routes, 650-651, 659-660
successors, 646
timers, 652
topology data, 657-658
global unicast addresses, 593
host configuration, 595
stateful DHCPv6, 596
stateless address autoconfiguration (SLAAC), 597
link-local addresses, 595
multicast addresses, 682
OSPF, 619-620
OSPFv3
configuration, 621-622
default routes, 627-628
interface cost metrics, 638-640
interfaces, 630
IPv6 MTU mismatches, 636-638
IPv6 routes, troubleshooting, 640-641
load balancing, 627
LSAs, 636
LSDBs, 636
multiarea on ABR configuration, 625
neighbors, 632
OSPFv2, compared, 621, 628-629
passive interfaces, 624
RIDs, 624
route selection metrics, 626
single-area configuration, 623-624
troubleshooting interfaces, 631-632
troubleshooting neighbors, 633-635
verifying interfaces, 630-631
verifying neighbors, 632-633
protocols, 619
QoS marking, 500
routers, enabling, 598
routes
EIGRP for IPv6 metrics, 650-651
OSPFv3 metrics, 626, 638-640
troubleshooting, 640-641
subnetting, 593
unique local unicast addresses, 593
static route configuration, 599
subnetting, 593-594
troubleshooting, 604
ACLs, 612
filtering issues, 604
host issues, 604
host pings fail from default router, 606-607
host pings only working in some cases, 605-606
missing IPv6 settings in host, 608-610
name resolution problems, 607-608
router issues, 604
routing, 611-612
unicast addresses, 593-595

ipv6 traffic-filter command, 673, 687

ipv6 unicast routing command, 598, 614

IS-IS (Integrated Intermediate System to Intermediate System), 175

ISL (Inter-Switch Link), 20-21, 525

ISPs (Internet service providers), 389

default routes, learning, 320-321

dial connections with PPP, 414

Internet edge, learning, 309

router configuration example, 419

subnets, advertising, 318

J

Jenkins continuous integration and automation tool, 744

jitter, managing, 491

K

keepalive failures, 355

keyboard, video display, or mouse (KVM), 733

keys (encryption), 395

keywords. ***See also*** **commands**

any, 448

deny, 442, 448-449

icmp, 481

log, 452, 670

permit, 442, 448-449

tcp, 464

udp, 464

knowledge gaps, finding, 792-793

K-values (EIGRP), 286

KVM (keyboard, video display, or mouse), 733

L

labs, completing, 795-796

LACP (Link Aggregation Control Protocol), 86

LANs, 523

defined, 16

DPs, 54, 104-105

interfaces, 490

redundancy

problems caused without STP, 45-46

STP, 42

security

IEEE 802.1x, 144-146

STP security exposures, 65-66

troubleshooting, 575-576

VLAN support, adding, 122

Layer 1

leased-line WANs

CSU/DSUs, 334

physical components, 332-333

speeds, 333-334

troubleshooting, 354

leased-line WANs with HDLC, 335-336

PPPoE

configuration, 416-417

switches, 21

troubleshooting, 427-428

Layer 2

leased-line WANs, 354-356

leased-lines with HDLC, 336

MLPPP, 349

PPPoE

configuration, 417

troubleshooting, 428-429

Layer 3
GRE tunnel issues, 409
leased-line WANs, troubleshooting, 357-358
MetroE design, 370
E-LAN service, 371-372
E-Line service, 370-371
E-Tree service, 372
MLPPP, 348-349
MPLS, 377
MPLS VPNs, 379-380
EIGRP challenges, 382
OSPF area design, 381-382
PPPoE
configuration, 417-418
status, verifying, 425
troubleshooting, 429
switches, 21
EtherChannels, 537-541
routed ports, 534-537
with SVIs, 529-534
VLAN (virtual LAN) routing, 23-24
LCP (Link Control Protocol), 341-342
learning state (interfaces), 58
leased-line WANs, 330-331
building, 335-336
CSU/DSU, 334
with HDLC, 336
configuring HDLC, 337-340
de-encapsulating/re-encapsulating IP packets, 336
framing, 336
physical components, 332-333
with PPP
authentication, 342-343
configuring PPP, 343-344
configuring PPP CHAP, 344-346
configuring PPP PAP, 346-347
control protocols, 341
framing, 341
multilink. See *MLPPP*
PPP functions, 340
speeds, 333-334
troubleshooting, 353-354
Layer 1 problems, 354
Layer 2 problems, 354-356
Layer 3 problems, 357-358
mismatched subnets, 358
least-bandwidth, 237
limiting SPAN sources, 725
Link Aggregation Control Protocol (LACP), 86
Link Control Protocol (LCP), 341-342
link-local addresses, 595
link-state advertisements. *See* LSAs
link-state database. *See* LSDB
link-state protocols, 175. *See also* OSPF
Link-State Update (LSU) packets, 183
links
access
MetroE, 365
MPLS, 378
addresses, 311-312
Ethernet, 185-186
RSTP types, 63
serial
bandwidth, 238-239
replacing with IP tunnels, 398
routing IP packets over, 398
list logic (IP ACLs), 444-445
listening state (interfaces), 58
LLQ (Low Latency Queuing), 505-507

load balancing

EIGRP, 263-264, 651-652

HSRP, 553

MLPPP, 349

OSPF, 217

OSPFv3, 627

local SPAN, configuring, 721-724

location (ACLs), 440-441

log keyword, 452, 670

log messages, unsolicited, 283

logging IPv6 ACLs, 670

logical switches, 157-158

logins (AAA), 147, 150

Long-Term Evolution (LTE), 393

loopback interfaces, 203

looping frames, preventing, 44

loss, managing, 491

Low Latency Queuing (LLQ), 505-507

LSAs (link-state advertisements), 183

exchanging with OSPF neighbors, 183-184

DRs on Ethernet links, 185-186

maintenance, 184-185

flooding, 179

LSDB relationship, 179

OSPFv3, 636

router, 636

LSDB (link-state database), 179

area design, 190

best routes, finding, 180

contents, displaying, 201

exchanging between neighbors

DRs on Ethernet links, 185-186

fully exchanging LSAs, 183-184

maintaining neighbors, 184-185

LSAs relationship, 179

OSPFv3, 636

LSU (Link-State Update) packets, 183

LTE (Long-Term Evolution), 393

M

mac-address command, 432

MAC addresses

burned-in, 49

forwarding, 111

learning, 111

tables

EtherChannel impact, predicting, 111-112

instability, 47

STP impact, predicting, 110

maintenance

EIGRP neighbors, 233

OSPF neighbors, 184-185

Managed Extensibility Framework (MEF), 366

Management Information Base. ***See*** **MIB**

management plane (networking devices), 764

managing

bandwidth, 491

delay, 491

IPv6 ACLs, 685

jitter, 491

loss, 491

SNMP, 695

manual EtherChannels configuration, 84-86

marking, 497-499

with classification, 497

DiffServ DSCP values

AF, 502-503

CS, 503

EF, 502

Ethernet 802.1Q headers, 500-501

Ethernet 802.11 headers, 501

IP headers, 499-501

MPLS Label headers, 501

trust boundaries, 501-502

matching packets, 441-442

matching parameters

extended numbered ACLs

protocol, source IP, and destination IP, 463-464

TCP and UDP port numbers, 464-467

standard numbered ACLs

any/all addresses, 448

command syntax, 445

exact IP address, 445-446

subset of address, 446-447

wildcard masks, 446-448

MaxAge timer (STP), 56

maximum-paths command, 218, 222, 270

EIGRP

for IPv4, 247, 647

for IPv6, 651, 662

load balancing, 263

OSPFv3, 627, 643

maximum transmission unit. *See* MTU

measuring

cloud computing services, 739

end-user traffic, 713

MEC (Multichassis EtherChannel), 161

MEF (Managed Extensibility Framework), 366

memory (TCAM), 766

messages

challenge, 342

debug, 261

EIGRP, 242

Get

agent information, 696

RO/RW communities, 699

SNMPv2 support, 699-701

ICMPv6

Echo request, 674

filtering, 668-669

NDP, filtering, 679-684

Inform, 696-697

SNMPv2, 701-702

SNMPv3, 710-711

NA (neighbor advertisement), 683

NS (neighbor solicitation), 683

OSPF Hello, 181-182

partial update, 232

RA (router advertisement), 610, 684

RS (router solicitation), 610, 684

RSTP, 62

Set

RO/RW communities, 699

SNMPv2 support, 699-701

writing variables on agents, 696

SNMP variables, monitoring, 696

STP Hello BPDU, 49

Trap, 696-697

SNMPv2, 701-702

SNMPv3, 710-711

unsolicited log, 283

update

BGP, 303, 310

DV routing protocols, 229-230

EIGRP, 235-236

metrics
BGP best path selection, 305-306
EIGRP, 236
bandwidth, 265
calculation, 236-237
components, 262
delay settings, 265
EIGRP topology database, 262
example, 237-238
FD (feasible distance), 240-241
RD (reported distance), 240-241
route load balancing, 264
serial link bandwidth, 238-239
IGP, 175-176
infinity, 231
IPv6 routes
EIGRP for IPv6, 650-651
OSPFv3 interface costs, 626
OSPF, 215
based on interface bandwidth, 216-217
higher reference bandwidth, 217
setting, 217
OSPFv3, 638-640
per-VLAN STP, 74
port, 78-79
root, 48
STP port, 53
MetroE (Metro Ethernet), 362-364
access links, 365
data usage, 373
bandwidth used, charging for, 373-374
overages, controlling, 374-375
IEEE Ethernet standards, 366
Layer 3 design, 370
E-LAN service, 371-372
E-Line service, 370-371
E-Tree service, 372
MEF, 366
physical design, 365-366
services, 366
E-LAN, 368-372
E-Line, 367-371
E-Tree, 369-372
topologies
full mesh, 368
hub and spoke, 369
partial mesh, 369
Point-to-Point, 367-368
MIB (Management Information Base), 695-697
OIDs, 697
variables
monitoring, 696
numbering/names, 697
views, 705
mind maps, reviewing, 795
mismatched IPv4 settings, troubleshooting, 568-569
mismatched masks, troubleshooting, 569-571
mismatched subnets, 286
MLPPP (multilink PPP), 348
configuring, 349-350
Layer 2 fragmentation balance, 349
Layer 3, 348-349
load balancing, 349
verifying, 351-353
monitor session command, 721, 728
monitoring MIB variables, 696
MPBGP (Multiprotocol BGP), 380

MPLS (Multiprotocol Label Switching), 362, 375-377
access links, 378
Label headers, 501
Layer 3 design, 377
public cloud connections, 747
QoS, 378-379
virtual private networks. *See* MPLS VPNs
MPLS VPNs (MPLS Virtual Private Networks), 376
EIGRP challenges, 382
Layer 3, 379-382
OSPF area design, 381-382
MST (Multiple Spanning Tree), 72
MTU (maximum transmission unit), 236
IPv6 mismatches, 636-638
OSPF mismatched settings, 296
mtu command, 432
multiarea on ABR OSPFv3 configuration, 625
multiarea OSPFv2 configuration, 206-210
network commands, 209
single-area configurations, 207-208
subnets, 206
verifying, 210-212
multiarea OSPFv3 configuration, 622
multicast addresses, 682
Multichassis EtherChannel (MEC), 161
multihomed Internet edge design, 306
multilayer switches. *See* Layer 3, switches
multilink interfaces, 349
multiple frame transmissions, 47
multiple queues (queuing systems), 504
multiple serial links between routers, 347
Multiple Spanning Tree (MST), 72
Multiprotocol BGP (MPBGP), 380
Multiprotocol Label Switching. *See* MPLS
multithreading, 734

N

NA (neighbor advertisement) messages, 683
name command, 25, 40, 135
named ACLs
configuration, 472
editing, 473-475
overview, 471-472
named mode (EIGRP configuration), 249
names (MIB variables), 697
National Institute of Standards and Technology (NIST), 739
native VLANs, 20
mismatched on trunks, 118
router configuration, 525-526
NBAR (Network Based Application Recognition), 498
NBIs (Northbound Interfaces), 768-770
NCP (Network Control Protocols), 341
NDA (nondisclosure agreement), 788
NDP (Neighbor Discovery Protocol), 593
filtering messages through IPv6 ACLs, 679-683
implicit filtering messages through IPv6 ACLs, 683-684
SLAAC, 597
ndp –an command, 615

neighbor commands, 322

neighbor shutdown command, 314

neighbors

advertisement (NA) messages, 683

BGP, 303

disabling, 314

states, 313

eBGP

configuring, 312

disabling, 314

using link addresses, configuring, 311

verifying, 312-313

EIGRP for IPv4, 234-235

discovery, 234

requirements, 286

status, 253

topology information, exchanging, 235-236

troubleshooting, 286-290

verifying, 235, 285-286

EIGRP for IPv6, 656-657

requirements, 656

troubleshooting, 656-657

OSPF

area mismatches, finding, 290-291

duplicate RIDs, 291-293

Hello/dead timer mismatches, 293-294

Hello messages, 181-182

LSDB exchange, 183-186

meeting, 181

requirements, 289

RIDs, learning, 181

states, 182-183, 186, 288

troubleshooting, 288-294

OSPFv3, 632

requirements, 633-634

troubleshooting, 633-635

verifying, 632-633

relationships, 284

neighbor requirements, 284

pinging routers, confirming, 285

routing protocol relationships, troubleshooting, 274

solicitation (NS) messages, 683

states, 628

netsh interface ipv6show neighbors command, 615

Network Based Application Recognition (NBAR), 498

network command, 222, 323

BGP table entries, injecting, 314

advertising subnets to ISPs, 318

classful network routes, 315-318

static discard routes, 319-320

EIGRP, 270

enabling, 246

for IPv4, 648

for IPv6 compatibility, 647

wildcard masks, 248

OSPF single-area configuration, 198-200

OSPFv2

interface configuration, 218

multiarea configuration, 209

Network Control Protocols (NCP), 341

network functions virtualization (NFV), 754

network interface cards (NICs), 718, 735

Network Interface Modules (NIMs), 332

Network Layer Reachability Information (NLRI), 303

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

Network Time Protocol (NTP), 757-758

networks

analyzers, 719

broad access, 739

classful

autosummarization at boundaries, 266-267

routes, injecting, 315-318

contiguous, 267

controllers

centralized control, 766-767

defined, 766

Northbound Interfaces (NBIs), 768-770

Southbound Interfaces (SBIs), 767-768

devices, 762

control, centralizing, 766-767

control plane, 763-764

data plane, 762-763

management plane, 764

security. See *authentication, AAA servers*

switch internal processing, 765-766

discontiguous, 267

discontiguous classful, 266-268

flow, 493

physical data center, 736

programmability, 760

APIC Enterprise Module (APIC-EM), 774-776

Application Centric Infrastructure (ACI), 773-774

comparisons, 776

public cloud

address assignment services, 756-757

DHCP services, 757

DNS services, 754-756

NTP, 757-758

VNFs, 752-754

redundancy needs, 547-548

traffic

bandwidth, managing, 491

characteristics, 491

delay, 491

jitter, 491

loss, 491

types, 492-494

unsecured, 400-401

virtual, 735-736, 754

VMs, 736

Nexus 1000v vSwitch, 736

NFV (network functions virtualization), 754

NHRP (Next Hop Resolution Protocol), 412-413

dynamic mapping, enabling, 412

spoke-to-spoke communication, 413

NICs (network interface cards), 718, 735

NIMs (Network Interface Modules), 332

NIST (National Institute of Standards and Technology), 739

NLRI (Network Layer Reachability Information), 303

NMS (Network Management Station), 695

notification community strings, 701

SNMP, 696-697

no auto-summary command, 268

no ip access-group command, 476

no ip address command, 539

no ip domain-lookup command, 572

no ip sla schedule 1 command, 715

no neighbor shutdown command, 314

no passive-interface command, 223, 270

no shutdown command, 40, 359

EIGRP for IPv6, 650, 662

Layer 1 leased-line WAN problems, 354

OSPF processes, 294

ROAS subinterfaces, 527

no spanning-tree portfast bpduguard default command, 95

no spanning-tree portfast default command, 95

no switchport command

Layer 3 EtherChannels, 539

Layer 3 switches, 543

routed ports, 535

nondisclosure agreement (NDA), 788

noninteractive data application traffic, 493

nonroot switches (RPs), 101-103

problems, troubleshooting, 103

tiebreakers, 102-103

normal-time questions, 785

Northbound Interfaces (NBIs), 768-770

notification community strings, 701

notifications

SNMP, 696-697

SNMPv3, 710-711

NS (neighbor solicitation) messages, 683

NTP (Network Time Protocol), 757-758

numbered ACLs, configuring, 475-476

numbers

AS numbers. *See* ASNs

HSRP group, 555

MIB variables, 697

ROAS subinterfaces, 525

sequence, editing ACLs with, 473-475

numeric reference table conversions

binary-to-hexadecimal, 808

decimal-to-binary, 805-807

hexadecimal-to-binary, 808

O

ODL (OpenDaylight), 771-772

Odom, Wendell Twitter/Facebook information, 799

OIDs (object IDs), 697

on-demand self-service (cloud computing), 739

one-way delay, 491

ONF (Open Networking Foundation), 771

Open SDN, 771

Open SDN Controller (OSC), 772

Open Shortest Path First. *See* OSPF

OpenDaylight (ODL), 771-772

OpenFlow, 768, 771

operations (IP SLAs), 713-715

OpFlex, 768

OSC (Open SDN Controller), 772

OSPF (Open Shortest Path First), 170, 179

area design, 189

ABR, 190, 210-211

areas, 189-190

backbone areas, 190

backbone routers, 190

benefits, 191

interarea routes, 190

internal routers, 190

intra-area routes, 190

MPLS VPNs, 381-382

network size, 189

problems, 188, 281

single-area, 188

SPF workload, reducing, 190

three-area, 189

best routes with SPF, calculating, 186-188

configuration

errors, troubleshooting, 282-283

mode, enabling, 198

default routes, 213-215

Dijkstra SPF algorithm, 180

EIGRP, compared, 224

goals, 302

Hello/dead timers, 293-294

history, 619

interarea routes, verifying, 212

interfaces

costs, setting, 216-217

EIGRP interfaces, compared, 281

identifying, 275

passive, 196

troubleshooting, 281-283

load balancing, 217

LSAs, 179

metrics, 215

based on interface bandwidth, 216-217

higher reference bandwidth, 217

setting, 217

MTU mismatched settings, 296

neighbors, 181

area mismatches, finding, 290-291

DRs on Ethernet links, 185-186

duplicate RIDs, 291-293

Hello messages, 181-182

Hello/dead timer mismatches, 293-294

LSAs, exchanging, 183-184

maintaining, 184-185

meeting, 181

requirements, 284, 289

RIDs, learning, 181

states, 182-186, 288

troubleshooting, 288-294

process-ids, 198

processes, shutting down, 294-296

RIDs

configuring, 203-204

duplicate, troubleshooting, 291-293

super backbone, 381

Version 2. *See* OSPFv2

OSPFv2 (OSPF Version 2), 170

default routes, 213-215

dual stack, 619

history, 619

interface configuration

example, 218

verifying, 219-221

load balancing, 217

metrics, 215

based on interface bandwidth, 216-217

higher reference bandwidth, 217

setting, 217

multiarea configuration, 206-210

network commands, 209

single-area configurations, 207-208

subnets, 206

verifying, 210-212

OSPFv3, compared, 621, 628-629

RIPv2/EIGRP, compared, 233

single-area configuration, 197-198

IPv4 addresses, 197

matching with network command, 198-200

multiarea configurations, 207-208

network command, 198

organization, 196-197

passive interfaces, 204-206

RIDs, 203-204

verifying, 200-202

wildcard masks, 199

OSPFv3 (OSPF Version 3), 616

address families dual stack, 620

configuration, 621

default routes, 627-628

load balancing, 627

multiarea example, 622

multiarea on ABR, 625

route selection metrics, setting, 626

single-area, 623-624

dual stack, 619

interfaces, 630

troubleshooting, 631-632

verifying, 630-631

IPv6

MTU mismatches, 636-638

routes, 638-641

LSAs, 636

LSDBs, 636

neighbors, 632

requirements, 633-634

troubleshooting, 633-635

verifying, 632-633

OSPFv2, compared, 621, 628-629

passive interfaces, 624

RIDs, 624

output queuing, 504

overages (MetroE data usage), 374-375

overlapping routes, troubleshooting, 577-580

overlapping subnets

with VLSM, 583-585

without VLSM, 581-583

P

PaaS (Platform as a Service), 743-744

packets

classification, 495

ACLs, 497

with marking, 497

matching, 496-497

NBAR, 498

router queuing, 496

routers, 497

congestion avoidance, 512

TCP windowing, 512-513

tools, 513-514

congestion management, 504

Low Latency Queuing (LLQ), 505-507

multiple queues, 504

output queuing, 504

prioritization, 505

queuing strategy, 507

round robin scheduling, 505

de-encapsulating/re-encapsulating with HDLC, 336

defined, 495

filtering. *See* ACLs

ICMPv6, 675

marking, 499

802.1Q headers, 500-501

802.11 headers, 501

with classification, 497

DiffServ DSCP AF values, 502-503

DiffServ DSCP CS values, 503

DiffServ DSCP EF values, 502

IP headers, 499-501

MPLS Label headers, 501

trust boundaries, 501-502

matching, 441-442

policing, 507

discarding excess traffic, 509

edge between networks, 509-510

features, 510

traffic rate versus configured policing rate, 508

router originated, 670

router queuing, 496

routing over serial links, 398

shaping, 507, 510

features, 512

slowing messages, 510

time intervals, 511-512

TCP, 675

UDP, 675

PAgP (Port Aggregation Protocol), 86

PAP (Password Authentication Protocol)

authentication, 343, 356

configuring, 346-347

parameters

ICMPv6, 669

ip_address, 198

wildcard_mask, 198

partial mesh topology (MetroE), 369

partial updates (EIGRP), 232, 235

passive-interface command, 205

defined, 222, 297

EIGRP, 251, 270

OSPF interfaces as passive, configuring, 196

OSPFv3, 624

passive-interface default command, 205, 270

passive interfaces

EIGRP, 251

OSPF, 196, 204-206

OSPFv3, 624

Password Authentication Protocol. *See* PAP

passwords, 698

path attributes (BGP), 305-306

Path MTU Discovery (PMTUD), 668

paths

forwarding

APIC-EM Path Trace ACL Analysis tool, 778

APIC-EM Path Trace app, 777

selections, 172

PBX (private branch exchange), 34

PCP (Priority Code Point) field (802.1Q header), 500

PE (provider edge), 377

Pearson Network Simulator (the Sim), 796

peers (BGPs), 303

periodic updates, 229

permit command, 471-474, 487

extended IPv6 ACLs, 675

GRE tunnel ACLs, 410

IPv6 ACLs, 672

permit gre command, 432

permit icmp any any router-advertisement command, 684

permit icmp any any router-solicitation command, 684

permit ipv6 commands, 687

permit keyword, 442, 448-449

Per-VLAN Spanning Tree Plus (PVST+), 72-73

physical data center networks, 736

physical design (MetroE), 365-366

physical server model, 734

ping command, 483, 571-574, 615

IPv6

connectivity, testing, 600-602

routes, testing, 614

leased-line WANs, 353

self-ping, 483-485

ping6 command, 615

IPv6 ACLs, 674

IPv6 connectivity, testing, 601

pings (IPv6 hosts)

failure from default router, 606-607

name resolution problems, 607-608

working only in some cases, 605-606

planes (networking devices)

control, 763-764

data, 762-763

management, 764

planning

EIGRP configuration, 246

VTP configuration, 129

Platform as a Service (PaaS), 743-744

PMTUD (Path MTU Discovery), 668

point-to-point edge ports, 63, 93

point-to-point GRE tunnels, 399

point-to-point lines, 330-331

building, 335-336

CSU/DSU, 334

with HDLC, 336

configuring HDLC, 337-340

de-encapsulating/re-encapsulating IP packets, 336

framing, 336

physical components, 332-333

with PPP

authentication, 342-343

configuring PPP, 343-344

configuring PPP CHAP, 344-346

configuring PPP PAP, 346-347

control protocols, 341

framing, 341

multilink. See *MLPPP*

PPP functions, 340

speeds, 333-334

troubleshooting, 353-354

Layer 1 problems, 354

Layer 2 problems, 354-356

Layer 3 problems, 357-358

mismatched subnets, 358

Point-to-Point over Ethernet. ***See*** **PPPoE**

point-to-point ports, 63, 93

Point-to-Point Protocol. ***See*** **PPP**

Point-to-Point topology (MetroE), 367-368

points of presence (PoP), 304, 365

policies

ACI, 773

filtering, 668

policing

data overages (MetroE), 374

QoS, 507

discarding excess traffic, 509

edge between networks, 509-510

features, 510

traffic rate versus configured policing rate, 508

rate, 508

pooling resources, 739

PoP (points of presence), 304, 365

Port Aggregation Protocol (PAgP), 86

PortChannels. ***See*** **EtherChannels**

PortFast, 65

configuring, 81

enabling/disabling, 83

global settings, displaying, 83

verifying, 82-83

ports

802.1w RSTP roles, 60

alternate, 60-61, 91-92

backup, 60, 91-92

blocking, choosing, 44

channels, 86

costs

IEEE default, 55

STP, 53, 78-79

designated, 49, 54, 60

disabled, 60

Layer 3 switch routed, 534-537

numbers, matching, 464-467

per-VLAN STP costs, 74

root (RPs), 60

nonroot switches, 101-103

switches, choosing, 52-53

RSTP

backup, 62-63

roles, 60, 91-92

states, 92-93

types, 63, 92

SPAN destination/source, 719

stacking ports, 156

states

RSTP, 92

STP versus RSTP, 62

switch root, choosing, 52-53

trusted/untrusted, 151-153

configuring, 153

DHCP snooping, 154

powers of 2 numeric reference table, 810

PPP (Point-to-Point Protocol), 340, 413

authentication, 342-343

CHAP

authentication, 342, 356

configuring, 344-345

verifying, 345-346

configuring, 343-344

control protocols, 341

dial connections to ISPs, 414

framing, 341

leased-line WANs, 340

multilink (MLPPP), 348

configuring, 349-350

Layer 2 fragmentation balance, 349

Layer 3, 348-349

load balancing, 349
verifying, 351-353
PAP
authentication, 343, 356
configuring, 346-347
PPPoE Layer 2 configuration, 417
status, 344
ppp authentication chap command, 345
ppp authentication command, 349, 359
ppp chap hostname command, 432
ppp chap password command, 432
ppp multilink command, 350, 360
ppp multilink group command, 360
ppp multilink group 1 command, 350
ppp pap sent-username command, 346, 359
PPPoE (Point-to-Point over Ethernet), 413-415
configuring, 415-416
ISP router configuration example, 419
Layer 1, 416-417
Layer 2, 417
Layer 3, 417-418
summary, 418-419
enabling, 417
history, 414
troubleshooting, 425-426
customer router configuration, 426
dialer 2 status, 427
Layer 1, 427-428
Layer 2, 428-429
Layer 3, 429
summary, 430
verification, 420-421
dialers, 421-422
Layer 3 status, 425
session status, 424
virtual-access interfaces, 423
pppoe-client dial-pool number command, 417, 432
pppoe enable command, 417, 432
practice exams
answering questions, 790-791
CCNA R&S, 790
checklist, 790
ICND2, 790
knowledge gaps, finding, 792-793
other, 792
scores, 796-797
taking, 789-790
preemption (HSRP active/standby roles), 557-558
pre-exam suggestions, 786-787
prefixes
BGP, 303
IPv6, 594, 670
preparing for the exam
CLI skills, 794-796
exam-day suggestions, 787
knowledge gaps, finding, 792-793
practice exams
answering questions, 790-791
CCNA R&S, 790
checklist, 790
ICND2, 790
other, 792
scores, 796-797
taking, 789-790
pre-exam suggestions, 786-787
preparing for failure, 788

question types, 784
ready to pass assessment, 797
study tasks, 798
studying after failing to pass, 797-798
tutorial, 784-785

prioritization (congestion management), 505

Priority Code Point (PCP) field (802.1Q header), 500

priority queues, 506

priv keyword (snmp-server group command), 707

private branch exchange (PBX), 34

private cloud computing, 739-741

private WANs

MetroE, 364
access links, 365
data usage, 373-375
E-LAN services, 368-372
E-Line services, 367-371
E-Tree services, 369-372
full mesh topology, 368
hub and spoke topology, 369
IEEE Ethernet standards, 366
Layer 3 design, 370-372
MEF, 366
partial mesh topology, 369
physical design, 365-366
Point-to-Point topology, 367-368
services, 366
MPLS, 375-377
access links, 378
Layer 3 design, 377
MPLS VPNs, 379-382
QoS, 378-379
VPNs, 376

public cloud
accessing, 746-749
branch office connections, 751
types, 362

probes, 713-715

process-ids (OSPF), 198

processes

OSPF, shutting down, 294-296
RSTP, 62

programmability (network), 760

APIC Enterprise Module (APIC-EM), 774-776
Application Centric Infrastructure (ACI), 773-774
comparisons, 776

proprietary routing protocols, 175

protocols, 224

BGP, 174, 300, 303
AS, 304
ASNs, 304
best path selection, 305-306
configuring, 310
external. See *eBGP*
IGPs, compared, 302
internal (iBGP), 304
ISP default routes, learning, 320-321
neighbors, 303, 313-314
prefixes, 303
reachability, 302
route advertising, 303-304
routing table analysis reports website, 303
table entries, injecting, 314-320
update messages, 303-310
BPDUs (bridge protocol data units), 49

CHAP
- *authentication, 342, 356*
- *configuring, 344-345*
- *verifying, 345-346*

control plane, 764

DHCP
- *Binding Table, 153*
- *DHCP Relay, 573*
- *public cloud services, 757*
- *snooping, 151-154*

Dijkstra SPF algorithm, 180

DTP, 116

DV (distance vector), 175, 228
- *distance/vector information learned, 228*
- *EIGRP as, 232-233*
- *route poisoning, 231-232*
- *split horizon, 230-231*
- *update messages, 229-230*

EAP, 146

EAPoL, 146

eBGP, 304
- *Internet edge, 306-309*
- *neighbors, 311-314*

EGP, 173, 302

EIGRP, 175

FHRP, 544
- *features, 550*
- *HSRP.* See *HSRP*
- *need for, 549*
- *options, 550-551*

GLBP, 544

HDLC, 331, 336-340, 398

HSRP, 544, 551
- *active/passive model, 551*
- *active/standby routers, choosing, 555*
- *active/standby rules, 557*
- *configuring, 554*
- *failover, 552*
- *group numbers, 555*
- *load balancing, 553*
- *no preemption, 557*
- *with preemption, 558*
- *troubleshooting, 560-563*
- *verifying, 555-556*
- *versions, 559-560*

iBGP, 304

IGPs, 173, 226
- *BGPs, compared, 302*
- *classless/classful, 177*
- *configuring, 310*
- *goals, 302*
- *metrics, 175-176*
- *routing protocol algorithm, 175*
- *subnets, 303*

IGRP, 175

IPv4. *See* IPv4 routing

IPv6. *See* IPv6 routing

link-state, 175

management plane, 765

matching, 463-464

MPBGP, 380

NDP, 593
- *filtering messages through IPv6 ACLs, 679-683*
- *implicit filtering messages through IPv6 ACLs, 683-684*
- *SLAAC, 597*

NHRP, 412-413
- *dynamic mapping, enabling, 412*
- *spoke-to-spoke communication, 413*

NTP, 757-758

OSPF. *See* OSPF

OSPFv2. *See* OSPFv2

OSPFv3. *See* OSPFv3

PAgP, 86

PAP

authentication, 343, 356

configuring, 346-347

PPP. *See* PPP

PPPoE, 413, 415

configuring, 415-419

enabling, 417

history, 414

ISP router configuration example, 419

troubleshooting, 425-430

verification, 420-425

RADIUS, 146-148

RIP, 175-176, 226

RIPv2, 302

EIGRP/OSPFv2, compared, 233

goals, 302

routable, 172

routed, 172

routing

administrative distance, 177-178

algorithms, 175

AS, 174

autosummarization, 266-268

classless/classful, 177, 266

convergence, 173

defined, 172

DV. See *DV protocols*

EGP (exterior gateway protocol), 173

functions, 172-173

IGP, 173-177

interfaces enabled with, verifying, 274

interior comparison, 233

IPv4, 202

link-state, 175

path selections, 172

proprietary, 175

RIPv1, 226

RIPv2, 226

route redistribution, 177

troubleshooting, 273-274

RSTP

alternate ports, 60-61

backup port role, 62-63

Cisco Catalyst STP modes, 88-90

implementing, 88

link types, 63

port roles, 60, 91-92

port states, 62, 92-93

port types, 63, 92

processes, 62

standards, 58

STP, compared, 59-60

RTP, 235

SNMP. *See* SNMP

STA (spanning-tree algorithm), 48

STP. *See* STP

TACACS+, 148

TCP

BGP connections, displaying, 313

packets, 675

port numbers, matching, 464-467

transporting messages between BGP peers, 310

windowing, 512-513

UDP

Jitter probes, 713

packets, IPv6 ACL matching, 675

port numbers, matching, 464-467

VRRP, 544

VTP, 120

automated update powers, 120

configuration, 129-131

domains, 125-127

features, 128

planning configuration, 129

pruning, 127-128

requirements, 126-127

servers, 124

standard range VLANs, 123

storing configuration, 134-135

switches synchronization to VLAN database, verifying, 131-133

synchronization, 125-126

transparent mode, 135

troubleshooting, 135-139

versions, 127

VLAN support, adding, 123

provider edge (PE), 377

pruning (VTP), 127-128

public cloud computing, 741

accessing with

Internet, 745-746

private WANs, 746-749

VPNs, 747

address assignment services, 756-757

branch offices example, 749-752

email services traffic flow, 750-751

Internet connections, 751

private WAN connections, 751

DHCP services, 757

DNS services, 754-756

intercloud exchanges, 748-749

NTP, 757-758

VNFs, 752-754

PVST+ (Per-VLAN Spanning Tree Plus), 72-73

Q

QoE (Quality of Experience), 492

QoS (Quality of Service), 378, 488

bandwidth, 491

classification, 495

ACLs, 497

with marking, 497

matching, 496-497

NBAR, 498

router queuing, 496

routers, 497

congestion avoidance, 512

TCP windowing, 512-513

tools, 513-514

congestion management, 504

Low Latency Queuing (LLQ), 505-507

multiple queues, 504

output queuing, 504

prioritization, 505

queuing strategy, 507

round robin scheduling, 505

defined, 488

delay, 491

jitter, 491

loss, 491

marking, 499
with classification, 497
DiffServ DSCP AF values, 502-503
DiffServ DSCP CS values, 503
DiffServ DSCP EF values, 502
Ethernet 802.1Q headers, 500-501
Ethernet 802.11 headers, 501
IP headers, 499-501
MPLS Label headers, 501
trust boundaries, 501-502
MPLS, 378-379
needs based on traffic types
data applications, 492-493
video applications, 494
voice applications, 493-494
policing, 507
discarding excess traffic, 509
edge between networks, 509-510
features, 510
traffic rate versus configured policing rate, 508
shaping, 507, 510
features, 512
slowing messages, 510
time intervals, 511-512
switches/routers, 495
tools, 496
VoIP, 493-494
query messages (EIGRP), 242
questions (exam)
answering, 790-791
budgeting time, 785
knowledge gaps, finding, 792-793
types, 784
queuing
congestion management, 504
Low Latency Queuing (LLQ), 505-507
multiple queues, 504
output queuing, 504
prioritization, 505
round robin scheduling, 505
strategy, 507
priority queues, 506
queue starvation, 506
routers, classification for, 496

R

RA (Router Advertisement), 610, 684
RADIUS protocol, 146-148
rapid elasticity (cloud computing), 739
Rapid PVST+, 72
Rapid Spanning Tree Protocol. *See* RSTP
rate limiting (DHCP snooping), 154
RD (reported distance), 240-241, 257
reachability (BGP), 302
read-only (RO) communities (SNMP), 699
read-write (RW) communities (SNMP), 699
ready to pass assessment (exam), 797
Real-time Transport Protocol (RTP), 235
redistribution
Internet edge ISP routes, learning, 309
routes (MPLS VPNs), 380
redundancy
FHRP
features, 550
HSRP. See *HSRP*

need for, 549

options, 550-551

LANs

problems caused without STP, 45-46

STP, 42

network needs for, 547-548

single points of failure, 547

reference bandwidth, 216-217

relationships (neighbors), 284

EIGRP for IPv6, 656-657

OSPFv3, troubleshooting, 633-635

pinging routers, confirming, 285

requirements, 284

states, 628

relay agents (DHCPv6), 596

Reliable Transport Protocol (RTP), 235

remark command, 472, 487

Remote SPAN (RSPAN), 721

reply messages (EIGRP), 242

reported distance (RD), 240-241, 257

Representational State Transfer (REST), 769

requirements

cloud computing services, 739

EIGRP for IPv6 neighbors, 656

neighbors, 284

EIGRP, 286

OSPF, 289

OSPFv3, 633-634

SNMPv3 configuration, 704

VTP, 126-127

resource pooling (cloud computing), 739

responders (IP SLAs), 713

REST (Representation State Transfer), 769

RESTful APIs, 769

reverse engineering from ACL to address range, 454-456

reversed source/destination IP address, troubleshooting, 480-481

RFC 1065, 694

RFC 4301 *Security Architecture for the Internet Protocol*, 395

RIDs (router IDs), 181

defining, 196

EIGRP, configuring, 252

OSPF, 181

configuring, 203-204

duplicate, troubleshooting, 291-293

OSPFv3, 624

RIP (Routing Information Protocol), 175-176, 226

RIPv2 (RIP Version 2), 226

EIGRP/OSPFv2, compared, 233

goals, 302

RO (read-only) communities (SNMP), 699

ROAS (router-on-a-stick), 520, 524

configuration, 524

example, 524

native VLANs, 525-526

subinterface numbers, 525

subinterfaces, creating, 524-525

troubleshooting, 528-529

verifying, 526-527

connected routes, 526

show vlans command, 527

subinterface state, 527

roles

ports

alternate, 60-61

backup, 62-63

root. See *RPs*

RSTP, 60, 91-92

STP, 57

root bridge IDs, 50

root costs (switches), 48

root ports. ***See*** **RPs**

root switches

electing, 50-52

election influence, configuring, 80-81

ruling out switches, 100-101

STP, verification, 77

troubleshooting, 99-101

round robin scheduling (queuing), 505

round-trip delay, 491

Round Trip Time (RTT), 715

routable protocols, 172

routed ports, 534-537

routed protocols, 172

Router Advertisement (RA) messages, 610, 684

router bgp command, 311

router eigrp command, 246, 270, 647

router-id command, 222, 614

OSPFv3, 624, 643

RIDs, defining, 196

router-on-a-stick. ***See*** **ROAS**

router ospf command, 196, 222

router ospf 1 command, 198

Router Solicitation (RS), 610

routers. ***See also*** **routes; routing**

ABR (Area Border Router), 190

interface OSPF areas, verifying, 210-211

OSPFv2 multiarea configuration, 209-210

advertisement (RA) messages, 610, 684

backbone, 190

best routes, finding, 180

classification, 497

ACLs, 497

NBAR, 498

Cloud Services Routers (CSRs), 747

configuring different VIPs, troubleshooting, 563

data plane processing, 763

designated (DRs), 185

backup (BDRs), 185

discovering, 211-212

Ethernet links, 185-186

DROthers, 186

flooding, 179

GRE tunnels between, 399

HSRP

active/passive model, 551

active/standby routers, choosing, 555

active/standby rules, 557

configuring, 554

failover, 552

group numbers, 555

load balancing, 553

no preemption, 557

with preemption, 558

troubleshooting, 560-563

verifying, 555-556

versions, 559-560

IDs. *See* RIDs

internal, 190, 623-624

IPv6

addressing configuration, 598-599

connectivity, verifying, 601-603

issues, 604

routing, enabling, 598

static route configuration, 599
troubleshooting, 611-612
ISP, 419
LSAs, 636
multiple serial links between, 347
OSPF interface costs, 216-217
public cloud networks, 754
QoS, 495
queuing
classification for, 496
congestion management, 504-507
strategy, 507
redundant, 549. *See also* FHRP
ROAS, 23, 524
configuration, 524-526
native VLANs, 525-526
subinterfaces, creating, 524-525
troubleshooting, 528-529
verifying, 526-527
router WAN interface status, 585
routing IP packets over serial links, 398
solicitation (RS) messages, 610, 684
troubleshooting
DHCP issues, 573-574
LAN issues, 575-576
VLAN routing, 21-23

routes. *See also* **routers; routing**
BGP
advertising, 303-304
best path selection, 305-306
classful networks, injecting, 315-318
default, 627-628
discard, 319
EIGRP
choosing, 234
load balancing, 263-264
tuning with bandwidth, 259
variance, 263-264
EIGRP for IPv6, 659-660
feasibility conditions, 242
feasible successor, 241-242
convergence, 260-261
identifying, 258-260
host, 357
interarea, 640
IPv6
EIGRP for IPv6 metrics, 650-651
OSFPv3 metrics, 626, 638-640
static, configuring, 599
troubleshooting, 640-641
ISP
default, learning, 320-321
Internet edge, learning, 309
OSPF
default routes, 213-215
interarea, verifying, 212
poisoning, 231-232
redistribution, 177, 380
static discard, 319-320
successor, 257-258

routing. *See also* **routers; routes**
EIGRP for IPv6, enabling/disabling, 650
LANs, 523
protocols. *See* routing protocols
troubleshooting
default router IP address setting, 572
DHCP issues, 573-574
DNS problems, 571-572
incorrect addressing plans, 581-585
IP forwarding issues, 577-580

LAN issues, 575-576

mismatched IPv4 settings, 568-569

mismatched masks, 569-571

router WAN interface status, 585

VLAN. *See* VLAN routing

Routing Information Protocol (RIP), 175

routing protocols

administrative distance, 177-178

algorithms, 175

AS, 174

autosummarization, 266

classful network boundaries, 266-267

discontiguous classful networks, 267-268

classless/classful, 177, 266

convergence, 173

defined, 172

DV, 175, 228

distance/vector information learned, 228

EIGRP as, 232-233

route poisoning, 231-232

split horizon, 230-231

update messages, 229-230

EGP (exterior gateway protocol), 173

functions, 172-173

IGP, 173

algorithms, 175

classless/classful, 177

metrics, 175-176

interfaces enabled with, verifying, 274

interior comparison, 233

IPv4, 202

link-state, 175

path selections, 172

proprietary, 175

RIPv1, 226

RIPv2, 226

route redistribution, 177

troubleshooting

configuration errors, 274

internetwork, analyzing, 273

neighbor relationships, 274

routing tables, 273

RPs (root ports), 60

nonroot switches, 101-103

problems, troubleshooting, 103

tiebreakers, 102-103

switches, choosing, 52-53

RS (Router Solicitation) messages, 610, 684

RSPAN (Remote SPAN), 721

RSTP (Rapid Spanning Tree Protocol), 58-59

alternate ports, 60-61

backup port role, 62-63

Cisco Catalyst switch RSTP modes, 88-90

implementing, 88

link types, 63

ports

roles, 60, 91-92

states, 62, 92-93

types, 63, 92

processes, 62

standards, 58

STP, compared, 59-60

RTP (Real-time Transport Protocol), 235

RTP (Reliable Transport Protocol), 235

RTT (Round Trip Time), 715

rules

AAA login authentication, 150

HSRP active/standby, 557

implicit IPv6 ACL ICMPv6 message filtering, 683-684

ruling out switches, 100-101

RW (read-write) communities (SNMP), 699

S

SaaS (Software as a Service), 743

SBIs (Southbound Interfaces), 767-768

scoring exams, 796-797

sdm prefer command, 532

sdm prefer lanbase-routing command, 543

SDN (Software Defined Networking), 760

APIC Enterprise Module (APIC-EM), 774-776

Application Centric Infrastructure (ACI), 773-774

architecture, 770

comparisons, 776

controllers

centralized control, 766-767

Northbound Interfaces (NBIs), 768-770

OpenDaylight SDN controller, 771

Southbound Interfaces (SBIs), 767-768

Open SDN, 771

Open SDN Controller (OSC), 772

OpenDaylight (ODL), 771-772

OpenFlow, 771

Secure Shell (SSH), 765

Secure Sockets Layer (SSL), 396-397

security

AAA servers

configuration, 148-150

login authentication rules, 150

login process, 147

TACACS+/RADIUS protocols, 148

access, 145

attacks

DHCP-based, 152

types, 150

authentication

802.1x, 145

AAA servers, 147-150

Internet VPNs, 393

SNMPv3, 699, 707-708

DHCP snooping

configuration settings, 153

DHCP-based attacks, 152

DHCP Binding Table, 153

features, 151

ports as trusted, configuring, 153

rate limiting, 154

rules summary, 153

trusted/untrusted ports, 151-154

encryption, 699, 707-708

IEEE 802.1x, 144-146

AAA servers, configuring, 145

authentication process, 145

EAP, 146

username/password combinations, verifying, 145

Internet VPNs, 393

IPsec encryption, 395-396

SNMP, 698-699

SNMPv3, 705-707

STP, 65-66

self-ping, 483-485

sender's bridge IDs, 50

sender's root cost, 50

sequence numbers, 473-475

serial cables, 332

serial links. ***See*** **leased-line WANs**

servers

AAA

authentication, 147-150

configuring for 802.1x, 145

defining, 149

enabling, 149

username/passwords, verifying, 145

Cisco hardware, 732-733

defined, 732

physical server model, 734

virtualization, 734-735

hosts, 734

hypervisors, 734

multithreading, 734

networking, 736

virtual data centers, 735-738

VMs, 734

VTP, 124

service-level agreements (SLAs), 712

service providers (SPs), 362

services

cloud computing

broad network access, 739

cloud services catalogs, 740

Infrastructure as a Service (IaaS), 742

measured, 739

on-demand self-service, 739

Platform as a Service (PaaS), 743-744

private, 739-741

public, 741

rapid elasticity, 739

requirements, 739

resource pooling, 739

Software as a Service (SaaS), 743

DHCP, 757

DNS, 754-756

Internet as WAN, 389

MetroE, 366

E-LAN, 368-372

E-Line, 367-371

E-Tree, 369-372

public cloud

accessing with Internet, 745-746

accessing with private WANs, 746-749

accessing with VPNs, 747

address assignment, 756-757

branch offices example, 749-752

intercloud exchanges, 748-749

session keys, 395

session status (PPPoE), 424

sessions (SPAN), 720-721, 725

Set messages

RO/RW communities, 699

SNMPv2 support, 699-701

writing variables on agents, 696

shaping (QoS), 507, 510

features, 512

rate, 510

slowing messages, 510

time intervals, 511-512

shaping data overages (MetroE), 375

shared edge ports, 93

shared keys, 395

shared ports, 63, 93

shared session keys, 395

shorter VLAN configuration example, 28-29

Shortest Path First algorithm. *See* SPF algorithm

show access-list command, 473

show access-lists command, 450, 457, 479, 487, 687

show arp command, 572

show commands

IPv6 ACLs, 673

routing protocol-enabled interfaces, verifying, 275

STP status, 68

show controllers command, 352

show controllers serial command, 360

show etherchannel 1 summary command, 86

show etherchannel command, 96, 543

show etherchannel summary command, 107, 540

show interfaces command, 298, 360, 543, 569

EIGRP neighbor requirements, verifying, 286

MLPPP, 352

OSPF

interfaces, 283

neighbors, 289

OSPFv3 interface bandwidth, 640

PPP CHAP status, 345

PPP PAP, 346

PPP status, 344

routed ports, 536

show interfaces description command, 298, 576

show interfaces dialer command, 421, 433

show interfaces status command

Layer 3 EtherChannels, 539

routed ports, 536

show interfaces switchport command, 31-34, 37, 41, 114-116, 135

show interfaces trunk command, 32-34, 38, 41, 116-117

show interfaces tunnel command, 405, 433

show interfaces virtual-access command, 433

show interfaces virtual-access configuration command, 423

show interfaces vlan command, 543

show ip access-list command, 457, 474-476

show ip access-lists command, 450, 479, 487

show ip bgp command, 323

show ip bgp summary command, 313, 323

show ip eigrp interfaces command, 271, 297

EIGRP-enabled interfaces, 250-251, 275

EIGRP neighbor requirements, verifying, 286

multilink interfaces, 352

show ip eigrp interfaces detail command, 250, 271

show ip eigrp neighbors command, 271, 297

neighbor status, displaying, 253

neighbor verification checks, 285

show ip eigrp topology all-links command, 260

show ip eigrp topology command, 271

feasible successor routes, 259

metrics, 262

successor routes, 258

topology table, 256

show ip interface brief command, 360

GRE tunnels, 404

multilink interfaces, 352

OSPF interfaces, troubleshooting, 283

show ip interface command, 286, 450, 457, 479

show ip ospf command, 223, 298

duplicate OSPF RIDs, 291

OSPF neighbors, troubleshooting, 289

show ip ospf database command, 179, 201, 223

show ip ospf interface brief command, 205, 223, 298

OSPF areas for ABR interfaces, 210

OSPF-enabled interfaces, identifying, 275

OSPF neighbors, troubleshooting, 289

OSPF status on interfaces, 281

OSPFv2 interface configuration, 221

show ip ospf interface command, 223, 298

DRs/BDRs details, displaying, 211

Hello/dead timer mismatches, 293

OSPF areas for ABR interfaces, 210

OSPF neighbors, troubleshooting, 289

OSPFv2 interface configuration, 220

passive interface, 206

show ip ospf neighbor command, 182, 223, 298

DRs/BDRs details, displaying, 211

neighbors, listing, 288

OSPF processes shutdown, 295

show ip ospf neighbor interface brief command, 295

show ip protocols command, 223, 271, 297

EIGRP-enabled interfaces, 251-252, 275

EIGRP neighbors, 253, 286

IPv4 routing protocols, 202

OSPF configuration errors, 282-283

OSPFv2 interface configuration, 219

show ip route command, 223, 271, 323, 577-580

administrative distance, 178

dialer interface Layer 3 orientation, 425

EIGRP-learned routes, displaying, 254

IPv4 routes added by OSPF, 201

routing tables, displaying, 543

show ip route eigrp command, 254, 271, 297

show ip route ospf command, 223, 298, 577-578

show ip route static command, 214

show ip sla enhanced-history distribution-statistics command, 729

show ip sla history command, 717, 729

show ip sla statistics command, 729

show ip sla summary command, 729

show ipv6 access-list command, 677, 687

show ipv6 eigrp interfaces command, 654, 662

show ipv6 eigrp interfaces detail command, 662

show ipv6 eigrp neighbors command, 663

show ipv6 eigrp topology command, 663

show ipv6 eigrp topology | section command, 663

show ipv6 interface command, 614, 687

show ipv6 neighbors command, 614

IPv6 ACL ICMPv6 NDP message filtering, 681

IPv6 IPv4 replacement, 603

show ipv6 ospf command, 640, 643

show ipv6 ospf database command, 636, 643

show ipv6 ospf interface brief command, 630, 640, 643

show ipv6 ospf interface command, 630-631, 643

show ipv6 ospf neighbor command, 635, 643

show ipv6 protocols command, 614, 643

EIGRP for IPv6, 662

EIGRP for IPv6 interfaces, 654

OSPFv3 interfaces, 630

show ipv6 route command, 614, 643

EIGRP for IPv6, 663

IPv6 router connectivity, 603

show ipv6 route eigrp command, 663

show ipv6 route ospf command, 638, 643

show ipv6 route | section command, 663

show ipv6 routers command, 614, 681

show mac address-table command, 114

show mac address-table dynamic command, 111

show monitor detail command, 724, 729

show monitor session all command, 723

show monitor session command, 724, 729

show ppp all command, 346-347, 360

show ppp multilink command, 353, 360

show pppoe session command, 424, 433

show running-config command, 135, 449, 473-475

show snmp command, 703, 729

show snmp community command, 702, 728

show snmp contact command, 728

show snmp group command, 709, 729

show snmp host command, 702, 729

show snmp location command, 728

show snmp user command, 708, 729

show spanning-tree bridge command, 81

show spanning-tree command, 96

show spanning-tree interface command, 96

show spanning-tree interface detail command, 82

show spanning-tree root command, 77, 81

show spanning-tree summary command, 83, 96

show spanning-tree vlan 10 bridge command, 77

show spanning-tree vlan 10 command, 75-77

show spanning-tree vlan 10 interface gigabitethernet0/2 state command, 92

show spanning-tree vlan command, 96

show standby brief command, 555-565

show standby command (HSRP), 565

configuration, 560

status, 556

show tcp brief command, 313

show tcp summary command, 323

show vlan brief command, 26-29, 114

show vlan command, 41, 114, 141

show vlan id command, 27, 114

show vlan status command, 135

show vlans command, 527, 543

show vtp password command, 134, 141

show vtp status command, 29, 41, 131, 134, 141

shutdown command, 40, 359

- EIGRP for IPv6, 650, 662
- Layer 1 leased-line WAN problems, 354
- OSPF processes, 294
- ROAS subinterfaces, 527

shutdown vlan command, 135, 140

shutting down OSPF processes, 294-296

signatures, 498

the Sim (Pearson Network Simulator), 796

Simple Network Management Protocol. *See* SNMP

single-area OSPF, 188

single-area OSPFv2 configuration, 197-198

- IPv4 addresses, 197
- matching with network command, 198-200
- multiarea configurations, 207-208
- network command, 198
- organization, 196-197
- passive interfaces, 204-206
- RIDs, 203-204
- verifying, 200-202
  - *IPv4 routing protocols, 201-202*
  - *LSDB contents, displaying, 201*
- wildcard masks, 199

single-area OSPFv3 configuration, 623-624

single homed Internet edge design, 306

single points of failure, 547

site-to-site VPNs, 394-396

SLA (service level agreement), 712

SLAAC (stateless address autoconfiguration)

- EUI-64, 597
- IPv6 settings, 597
- NDP, 597
- troubleshooting, 609-610

SLBaaS (SLB as a service), 753

SNMP (Simple Network Management Protocol), 692

- agents, 695-696
- clear-text passwords, 698
- communities, 698-699
- Get messages
  - *agent information, 696*
  - *RO/RW communities, 699*
  - *SNMPv2 configuration, 699-701*
- history, 695
- Inform messages, 696-697, 701-702
- managers, 695
- MIB, 696-697
- notifications, 696-697
- read-only (RO) communities, 699
- read-write (RW) communities, 699
- security, 698-699
- Set messages
  - *RO/RW communities, 699*
  - *SNMPv2 configuration, 699-701*
  - *writing variables on agents, 696*
- Trap messages, 696-697, 701-702

snmp-server command, 700

snmp-server community command, 727

snmp-server contact command, 727

snmp-server enable traps command, 727

snmp-server group command, 705

snmp-server host command, 701, 710, 727

snmp-server location command, 727

snmp-server user command, 707

SNMPv2

configuring

Get/Set messages, 699-701

Trap/Inform messages, 701-702

verifying, 702-704

security, 699

SNMPv2c (Community-based SNMP Version 2), 699

SNMPv3

configuring, 704

authentication, 707-708

encryption, 707-708

groups, 705-707

notifications, 710-711

requirements, 704

summary, 711-712

users, 707

verifying, 708-709

groups

MIB views, 705

security levels, 705

write views, 706

Inform messages, 710-711

MIB views, 705

security, 699

Trap messages, 710-711

Software as a Service (SaaS), 743

Software Defined Networking. ***See*** **SDN**

solution apps, 777

sources

addresses, 406

IPs, matching, 463-464

IP SLAs, 713

ports (SPAN), 719

SPAN, limiting, 725

Southbound Interfaces (SBIs), 767-768

SPAN (Switched Port Analyzer), 718

dependencies, 722

destination ports, 719

Encapsulated RSPAN (ERSPAN), 721

local, 721-724

network analyzer needs for, 719

Remote (RSPAN), 721

sessions, 720-721

source ports, 719

sources, limiting, 725

traffic direction, 725

VLANs, monitoring, 721

spanning-tree algorithm (STA), 48

spanning-tree bpduguard disable command, 95

spanning-tree bpduguard enable command, 81, 95

spanning-tree bpguard enable command, 75

spanning-tree commands, 95

spanning-tree mode command, 88, 95

spanning-tree mode mst command, 72

spanning-tree mode pvst command, 72

spanning-tree mode rapid-pvst command, 72, 90

spanning-tree pathcost method long command, 55

spanning-tree portfast bpduguard default command, 95

spanning-tree portfast command, 75, 81, 95

spanning-tree portfast default command, 83, 95

spanning-tree portfast disable command, 83, 95

Spanning Tree Protocol. *See* STP

spanning-tree vlan 10 port priority 112 command, 103

spanning-tree vlan command, 74

speed command, 576

speeds

LAN/WAN interfaces, 490

leased-line WANs, 333-334

SPF (Shortest Path First) algorithm, 180

Dijkstra SPF, 180

OSPF best routes, calculating, 186-188

spinning up VMs, 742

split horizon (DV routing protocols), 230-231

spoofing, 422

SPs (service providers), 362

SSH (Secure Shell), 765

SSL (Secure Sockets Layer), 396-397

STA (spanning-tree algorithm), 48

stack masters, 157

stacking cables, 156

stacking modules, 156

stacking ports, 156

stacking switches

access layer switches, 156-157

benefits, 155

chassis aggregation, 159-161

FlexStack/FlexStack-Plus, 158

operating as single logical switch, 157-158

stack masters, 157

standard ACLs, configuring, 671-674

standard numbered IPv4 ACLs, 443

access-list command, 454

command syntax, 445

configuration examples, 448-452

list logic, 444-445

matching any/all addresses, 448

matching exact IP address, 445-446

matching subset of address, 446-447

overview, 443

reverse engineering from ACL to address range, 454-456

troubleshooting, 452-453

verification, 452-453

wildcard masks

binary wildcard masks, 447-448

decimal wildcard masks, 446-447

standard range VLANs, 123

standby 1 preempt command, 558

standby command, 554, 564

standby HSRP routers, 557

standby version 1 | 2 command, 564

standby version command, 559

stateful DHCP, troubleshooting, 608-609

stateful DHCPv6, 596

stateless address autoconfiguration. *See* SLAAC

states

change reactions (STP topology), 55-56

discarding, 61

interfaces

changing with STP, 57-58

criteria, 48-49

forwarding/blocking, 47

learning, 58

listening, 58

neighbors

BGP, 313

OSPF, 182-183, 186, 288

OSPFv3, 632

relationships, 628

ports

RSTP, 92-93

STP versus RSTP, 62

ROAS subinterfaces, 527

STP, 57

tunnel interfaces, 407

VLAN mismatched trunking operational, 116

static discard routes, 319-320

static routes (IPv6), configuring, 599

status

BPDU Guard global settings, 83

EIGRP neighbors, 233, 253

HSRP, 555

interface codes, 353

PortFast global settings, 83

PPP, 344

PPP CHAP, 345

PPP PAP, 346

PPPoE

Layer 3, 425

sessions, verifying, 424

STP verification, 75-77

steady-state operation (STP), 56

STP (Spanning Tree Protocol), 42

802.1D standard, 58

behind the scenes summary, 72

BIDs

defined, 49

root switch election, 50-52

system ID extensions, 73-74

BPDUs (bridge protocol data units), 49

BPDU Guard

configuring, 81

enabling/disabling, 83

global settings, displaying, 83

verifying, 82-83

Cisco Catalyst switch STP modes, 88-89

configuration, 71

modes, 72

options, 74-75

per-VLAN port costs, 74

PVST+, 72-73

system ID extensions, 73-74

convergence, 48, 105-106

EtherChannels, 64-65

configuring, 84-87

MAC tables impact, predicting, 111-112

troubleshooting, 106-109

forwarding or blocking criteria, 48-49

interface states, changing, 57-58

LAN redundancy, 42-46

LAN segment DPs, choosing, 54

looping frames, preventing, 44

MAC tables impact, predicting, 110

PortFast, 65

configuring, 81

enabling/disabling, 83

global settings, displaying, 83

verifying, 82-83

ports
blocking, choosing, 44
costs, 53, 78-79
states, 62
purpose, 47-49
roles, 57
root election influence, configuring, 80-81
root switch election, 50-52, 100-101
RSTP (Rapid STP), 58-59
alternate ports, 60-61
backup port role, 62-63
Cisco Catalyst switch RSTP modes, 88-90
implementing, 88
link types, 63
port roles, 91-92
port states, 92-93
port types, 63, 92
processes, 62
standards, 58
STP, compared, 59-60
security, 65-66
STA (spanning-tree algorithm), 48
states, 56-57
switch reactions to changes, 56-57
switch RPs, choosing, 52-53
tiebreakers, 102-103
timers, 56-57
topology influences, 55-56
troubleshooting
convergence, 105-106
DPs on LAN segments, 104-105
root switch election, 99-101
RPs on nonroot switches, 101-103
verification, 75-77

studying after failing the exam, 797-798
studying for exam, 798
subinterfaces
defined, 524
ROAS
creating, 524-525
numbers, 525
state, verifying, 527
subnet masks
mismatched masks, troubleshooting, 569-571
VLSM (variable length subnet masking)
overlapping subnets, 583-585
recognizing when VLSM is used, 581
subnets
advertising to ISPs, 318
IGPs, 303
IPv6, 593-594
mismatched
EIGRP neighbors, 286
leased-line WANs, 358
OSPFv2 multiarea configuration, 206
overlapping subnets
with VLSM, 583-585
without VLSM, 581-583
subset of IP address, matching, 446-447
successors
EIGRP
identifying, 257-258
for IPv4, 241-242
for IPv6, 646
feasible
convergence, 260-261
identifying, 258-260

super backbone (OSPF), 381

superior Hello, 50

supplicants, 145

SVIs (switched virtual interfaces), 520, 529

- configuring, 529-531
- troubleshooting, 532-534
- verifying, 531

Switched Port Analyzer. ***See*** **SPAN**

switches

- as 802.1x authenticators, 145
- access layer, 156-157
- adding, 137-139
- chassis aggregation, 159
  - *benefits, 161*
  - *design, improving, 160*
  - *distribution/core switches high availability, 159-160*
  - *switch stacking, 159-161*
- Cisco Catalyst
  - *RSTP modes, 88-90*
  - *STP modes, 88-89*
- core, 159-160
- distribution
  - *design, improving, 160*
  - *high availability with chassis aggregation, 159-160*
- internal processing, 765-766
- Layer 2, 21
- Layer 3, 21
  - *with routed ports, 534-537*
  - *VLAN routing, 23-24*
- Layer 3 EtherChannels
  - *configuring, 537-539*
  - *troubleshooting, 541*
  - *verifying, 539-540*
- Layer 3 with SVIs
  - *configuring, 529-531*
  - *troubleshooting, 532-534*
  - *verifying, 531*
- links, 63
- logical, 157-158
- nonroot, 101-103
- PortFast, 65
- QoS, 495
- root
  - *costs, 48*
  - *electing, 50-52*
  - *election influence, configuring, 80-81*
  - *ruling out switches, 100-101*
  - *STP verification, 77*
  - *troubleshooting, 99-101*
- RPs (root ports), choosing, 52-53
- SPAN, 718
  - *dependencies, 722*
  - *destination ports, 719*
  - *Encapsulated RSPAN (ERSPAN), 721*
  - *limiting sources, 725*
  - *local, 721-724*
  - *network analyzer needs, 719*
  - *Remote (RSPAN), 721*
  - *sessions, 720-721*
  - *source ports, 719*
  - *traffic direction, 725*
  - *VLANs, monitoring, 721*
- stacking
  - *access layer switches, 156-157*
  - *benefits, 155*
  - *chassis aggregation, 159-161*
  - *FlexStack/FlexStack-Plus, 158*

operating as single logical switch, 157-158

stack masters, 157

synchronization to VLAN database, verifying, 131-133

ToR (Top of Rack), 736

traditional access switching, 155

virtual (vSwitches), 735

voice switches, 34

as VTP servers, 124

switchport access vlan command, 25, 28-29, 37-40, 113, 135

switchport command

Layer 3 switches, 543

routed ports, 535

switchport mode access command, 25, 28, 37-38, 139

switchport mode command, 30, 40

switchport mode dynamic auto command, 116

switchport mode dynamic desirable command, 32

switchport mode trunk command, 30, 116, 524

switchport nonegotiate command, 34, 40, 116, 139

switchport trunk allowed vlan command, 41, 117

switchport trunk encapsulation command, 30, 40

switchport trunk native vlan command, 40, 118

switchport voice vlan command, 36-38, 41, 135

synchronizing

switches, 131-133

VTP, 125-126, 136-137

system ID extensions (BIDs), 73-74

T

T1. *See* leased-line WANs

T3, 334

TACACS+, 148

tagging (VLAN), 18-20

tail drops, 513

TCAM (ternary content-addressable memory), 766

T-carrier systems, 333

TCP (Transmission Control Protocol)

BGP connections, displaying, 313

packets, 675

port numbers, matching, 464-467

transporting messages between BGP peers, 310

windowing, 512-513

tcp keyword, 464

TCP/IP networks, 694

TDM (time-division multiplexing), 334

telcos (telephone companies), 331, 390

Telnet, 765

ternary content-addressable memory (TCAM), 766

testing IPv6

ACLs, 677

connectivity

hosts, 600-601

routers, 601-603

three-area OSPF, 189

TID fields (QoS marking), 501

tiebreakers (STP), 102-103

time burners, 785

time-division multiplexing (TDM), 334

time (exam)

budget versus number of questions, 785

checking, 786

time intervals (QoS shaping), 511-512

timers

EIGRP for IPv6, 652

EIGRP neighbors, 233

Hello messages, 184

Hello/dead mismatches, troubleshooting, 293-294

STP, 56-57

tools

APIC-EM ACL Analysis, 777

APIC-EM Path Trace ACL Analysis tool, 777-778

APIC-EM Path Trace app, 777

QoS

ACLs, compared, 496

classification, 495-498

congestion avoidance, 512-514

congestion management, 504-507

marking, 499-503

policing, 507-510

queuing strategy, 507

shaping, 507-512

Top of Rack (ToR) switches, 736

topologies

EIGRP

displaying, 255-257

feasible successor routes, 258-261

metrics, 262

successor routes, identifying, 257-258

EIGRP for IPv6, 657-658

MetroE, 366

full mesh, 368

hub and spoke, 369

partial mesh, 369

Point-to-Point, 367-368

OSPF area design, 188

STP, influences, 55-56

ToR (Top of Rack) switches, 736

ToS (Type of Service) field (IPv4), 499

traceroute command, 574

GRE tunnels, 406

IPv6

connectivity, testing, 600-602

network router problems, troubleshooting, 611

routes, testing, 614

traceroute6 command, 615

tracert command, 615

traditional access switching, 155

traffic

bandwidth, managing, 491

characteristics, 491

congestion avoidance, 512

TCP windowing, 512-513

tools, 513-514

congestion management, 504

Low Latency Queuing (LLQ), 505-507

multiple queues, 504

output queuing, 504

prioritization, 505

round robin scheduling, 505

strategy, 507

delay, managing, 491

end-user, measuring, 713

IPv6 ACLs, 670

jitter, 491

loss, 491

policing, 507

discarding excess traffic, 509

edge between networks, 509-510

features, 510

traffic rate versus configured policing rate, 508

public cloud branch office email services, 750-751

shaping, 507, 510

features, 512

slowing messages, 510

time intervals, 511-512

SPAN sessions, 725

types

data, 492-493

video, 494

voice, 378, 493-494

Traffic Class field (IPv6), 500

Transmission Control Protocol. ***See*** **TCP**

transparent mode (VTP), 135

Trap messages, 696-697

SNMPv2, 701-702

SNMPv3, 710-711

troubleshooting

CHAP authentication failures, 356

DPs on LAN segments, 105

EIGRP for IPv6

interfaces, 655

neighbors, 656-657

routes, 660

EIGRP interfaces, 275

configuration problems, 278-281

working details, 276-278

EIGRP neighbors

authentication failures, 286

example, 286-288

incorrect ASNs, 288

mismatched subnets, 286

verification checks, 285-286

EtherChannels, 106

channel-group command incorrect options, 106-108

configuration checks before adding interfaces, 108-109

GRE tunnels, 406

ACLs, 409-410

interface state, 407

Layer 3 issues, 409

source/destination addresses, 406

tunnel destination, 408

HSRP, 560

ACL blocks HSRP packets, 563

configuration, 560-561

group number mismatches, 563

misconfiguration symptoms, 561

routers configuring different VIPs, 563

version mismatches, 562

with IP SLA

counters, 715-716

history data, 717

IPv4 ACLs, 477

ACL behavior in network, 477-479

ACL interactions with router-generated packets, 483-485

common syntax mistakes, 481

inbound ACL filters routing protocol packets, 481-482

reversed source/destination IP address, 480-481

troubleshooting commands, 479-480

IPv4 routing

default router IP address setting, 572

DHCP issues, 573-574

DNS problems, 571-572
incorrect addressing plans, 581-585
IP forwarding issues, 577-580
LAN issues, 575-576
mismatched IPv4 settings, 568-569
mismatched masks, 569-571
packet filtering with access lists, 586
router WAN interface status, 585
IPv6 routing, 604
ACLs, 612
filtering issues, 604
host issues, 604
host pings fail from default router, 606-607
host pings only working in some cases, 605-606
missing IPv6 settings in host, 608-610
name resolution problems, 607-608
router issues, 604
routes, 640-641
routing, 611-612
Layer 3 EtherChannels, 541
leased-line WANs, 353-354
Layer 1 problems, 354
Layer 2 problems, 354-356
Layer 3 problems, 357-358
mismatched subnets, 358
neighbors, 285
OSPF
MTU mismatched settings, 296
processes, shutting down, 294-296
OSPF interfaces, 281-283
area design, 281
configuration errors, 282-283
details, checking, 283
unsolicited log messages, 283
OSPF neighbors, 288-294
area mismatches, finding, 290-291
duplicate RIDs, 291-293
Hello timer/dead timer mismatches, 293-294
LAN problems, 289
neighbor states, 288
OSPFv3
interfaces, 631-632
neighbors, 633-635
PAP authentication failures, 356
PPPoE, 425-426
customer router configuration, 426
dialer 2 status, 427
Layer 1, 427-428
Layer 2, 428-429
Layer 3, 429
summary, 430
ROAS, 528-529
routing protocols
configuration errors, 274
internetwork, analyzing, 273
neighbor relationships, 274
routing tables, 273
routing with SVIs, 532-534
RP problems, 103
SPAN sessions, 725
standard numbered ACLs, 452-453

STP

convergence, 105-106

DPs on LAN segments, 104-105

root switch election, 99-101

RPs on nonroot switches, 101-103

switch data plane forwarding

EtherChannel impact on MAC tables, 111-112

STP impact on MAC tables, 110

VLAN of incoming frames, 112-113

VLANs

access interfaces, 113-114

frame switching problems, 113

undefined/disabled VLANs, 114-115

VLAN trunking

frame switching problems, 113

mismatched native VLANs, 118

mismatched operational states, 116

mismatched supported VLAN lists, 117-118

VTP, 135

adding switches, 137-139

common configuration rejections, 137

synchronization, 136-137

trunking (VLANs)

802.1Q, 20-21

configuration, 30-34

disabling, 139

ISL (Inter-Switch Link), 20-21

overview, 18

protocol. *See* VTP

troubleshooting, 113-118

VLAN tagging, 18-20

trust boundaries (QoS marking), 501-502

trusted ports, 151

configuring, 153

DHCP snooping, 154

tunnel destination command, 406-408, 432

tunnel mode gre ip command, 404, 432

tunnel mode gre multipoint command, 404

tunnel source command, 406-407, 432

tunnels

destinations, 408

GRE, 398

between routers, 399

configuring, 402-404

details, displaying, 404

functionality, testing, 406

large scale environments, 411

multipoint with DMVPN, 411

point-to-point, 399

routes, 405

troubleshooting, 406-410

tunnel interfaces, 398

unsecured networks, 400-401

verifying, 404-406

interfaces

ACLs, 409-410

creating, 400

destinations, 408

Layer 3 issues, 409

replacing serial links, 398

state, 407

VPN, 394-395

tutorial (exam), 784-785

Twitter (Wendell Odom), 799

Type of Service (ToS) field (IPv4), 499

U

UCS (Unified Computing System), 733

UDP (User Datagram Protocol)

- Jitter probes, 713
- packets, IPv6 ACL matching, 675
- port numbers, matching, 464-467

undebug all command, 298

undefined VLANs, troubleshooting, 114-115

unequal-cost load balancing, 263

UNI (user network interface), 365

unicast IPv6 addresses, 593-595

Unified Computing System (UCS), 733

unique local unicast addresses, 593

unsecured networks (GRE tunnels), 400-401

unsolicited log messages, 283

untrusted ports, 151-154

upd keyword, 464

updates

- BGP, 303, 310
- DV protocols, 229-230
- EIGRP, 235-236
- full, 229
- partial, 232
- periodic, 229

User Datagram Protocol. ***See*** **UDP**

user network interface (UNI), 365

username command, 345, 359

U.S. National Institute of Standards and Technology (NIST), 739

V

v1default MIB view, 706

variable length subnet masking. ***See*** **VLSM**

variables (MIB)

- monitoring, 696
- numbering/names, 697

variance (EIGRP), 263-264

variance command, 270

- EIGRP for IPv4, 247, 263, 647
- EIGRP for IPv6, 651, 662

vCPU (virtual CPU), 734

vector (DV protocols), 228

verification command, 75

verifying

- BPDU Guard, 82-83
- data and voice VLANs, 36-38
- eBGP neighbors, 312-313
- EIGRP configuration, 249
  - *EIGRP enabled interfaces, finding, 250-252*
  - *IPv4 routing table, displaying, 253-254*
  - *neighbor status, displaying, 253*
- EIGRP for IPv6
  - *interfaces, 654*
  - *routes, 659-660*
- EIGRP neighbors, 235, 285-286
- EtherChannel configuration before adding interfaces, 108-109
- GRE tunnels, 404-406
- HDLC, 339
- HSRP, 555-556
- interarea OSPF routes, 212

IPv6 connectivity, 600

hosts, 600-601

routers, 601-603

Layer 3 EtherChannels, 539-540

MLPPP, 351-353

OSPFv2 configurations

interfaces, 219-221

multiarea, 210-212

single-area, 200-202

OSPFv3

interfaces, 630-631, 638-640

neighbors, 632-633

PortFast, 82-83

PPP

CHAP, 345-346

PAP, 347

PPPoE, 420-421

dialers, 421-422

Layer 3 status, 425

session status, 424

virtual-access interfaces, 423

ROAS, 526-527

routing protocol-enabled interfaces, 274

routing with SVIs, 531

SNMPv2 configuration, 702-704

SNMPv3 configuration, 708-709

standard numbered ACLs, 452-453

STP, 75-77

switches synchronization to VLAN database, 131-133

username/passwords on AAA servers, 145

versions

HSRP, 559-560

OSPF, 619

VTP, 127

video traffic

QoS requirements, 494

shaping time intervals, 512

views (MIB), 705

virtual-access interfaces, 423

virtual LANs. *See* VLANs

virtual machines. *See* VMs

virtual network functions (VNFs), 752-754

Virtual Private LAN Service (VPLS), 367

Virtual Private Networks. *See* VPNs

Virtual Private Wire Service (VPWS), 367

Virtual Router Redundancy Protocol (VRRP), 544

virtualization

ASA firewall (ASAv), 754

CPU (vCPU), 734

data centers

networking, 735

physical networks, 736

vendors, 735

workflow, 737-738

firewalls, 754

machines. *See* VMs

network functions virtualization (NFV), 754

networks, 735-736, 754

NICs (vNICS), 735

routers (public cloud networks), 754

servers, 734-735

hosts, 734

hypervisors, 734

multithreading, 734

networking, 736

virtual data center vendors, 735

VMs, 734

switches (vSwitches), 735

VLANs (virtual LANs)

configuration

data and voice VLANs, 36-38

database, VTP synchronization, 125-126

full VLAN configuration example, 25-28

overview, 24-25

shorter VLAN configuration example, 28-29

trunking, 30-34

database, switches synchronization, 131-133

default, 25

enabling/disabling, 115

IDs, 18

incoming frames, choosing, 112-113

interfaces. *See* SVIs

IP telephony, 34

data and voice VLAN concepts, 34-36

data and voice VLAN configuration and verification, 36-38

summary, 38-39

LAN support, adding, 122

mismatched native on trunks, 118

mismatched supported trunk lists, 117-118

native, 20, 525-526

overview, 16-18

routing. *See* VLAN routing

SPAN monitoring, 721

standard range, 123

tagging, 18-20

troubleshooting

access interfaces, 113-114

frame switching process problems, 113

undefined/disabled VLANs, 114-115

trunking

802.1Q, 20-21

configuration, 30-34

disabling, 139

ISL (Inter-Switch Link), 20-21

overview, 18

protocol. See *VTP*

troubleshooting, 113-118

VLAN tagging, 18-20

vlan 10 command, 122

vlan 200 command, 137

vlan command, 25, 37, 40, 135

VLAN routing, 21

Layer 3 EtherChannels

configuring, 537-539

troubleshooting, 541

verifying, 539-540

Layer 3 switch routed ports, 23-24, 534-537

Layer 3 switching with SVIs

configuring, 529-531

troubleshooting, 532-534

verifying, 531

ROAS, 524

configuration, 524-526

troubleshooting, 528-529

verifying, 526-527

routers, 21-23

VLAN Trunking Protocol. *See* VTP

VLSM (variable length subnet masking)
overlapping subnets, 583-585
recognizing when VLSM is used, 581

VMs (virtual machines), 734
ACI, 773
IaaS, 742
networking, 736
PaaS, 743-744
SaaS, 743
spinning up, 742
virtual NICs (vNICs), 735

VNFs (virtual network functions), 752-754

vNICs (virtual NICs), 735

voice switches, 34

voice traffic, 493
QoS requirements, 494
shaping time intervals, 512
VoIP, 378

VoIP (Voice over IP), 378, 493-494

VPLS (Virtual Private LAN Service), 367

VPNs (Virtual Private Networks)
client, 396-397
dynamic multipoint (DMVPN), 411
multipoint GRE tunnels, 411
NHRP (Next Hop Resolution Protocol), 412-413
Internet, 389
benefits, 394
security, 393
MPLS VPNs, 376
EIGRP challenges, 382
Layer 3, 379-382
OSPF area design, 381-382
public cloud, accessing, 747
site-to-site, 394-396
tunnels, 394-395

VPWS (Virtual Private Wire Service), 367

VRRP (Virtual Router Redundancy Protocol), 544

vSwitches (virtual switches), 735

VTP (VLAN Trunking Protocol), 29, 120
automated update powers, 120
configuration
common rejections, troubleshooting, 137
default VTP settings, 129
example, 130-131
new VTP configuration settings, 130
planning, 129
steps, 129
storing, 134-135
domains, 125-127
features, 128
pruning, 127-128
requirements, 126-127
servers, 124
standard range VLANs, 123
switches synchronization to VLAN database, verifying, 131-133
synchronization, 125
transparent mode, 135
troubleshooting, 135
adding switches, 137-139
common configuration rejections, 137
synchronization, 136-137
versions, 127
VLAN support, adding, 123

vtp commands, 134

vtp domain command, 134, 140

vtp mode command, 40, 134, 140

vtp mode off command, 29, 135

vtp mode transparent command, 29, 135

vtp password command, 134, 140

vtp pruning command, 134, 140

vtp version command, 140

W – Z

WANs

Ethernet, 747

Frame Relay, 362

interface speeds, 490

Internet access, 389

Internet as WAN service, 389

leased-line, 330-331

building, 335-336

CSU/DSUs, 334

mismatched subnets, 358

physical components, 332-333

speeds, 333-334

troubleshooting, 353-358

leased-line with HDLC, 336

configuring HDLC, 337-340

de-encapsulating/re-encapsulating IP packets, 336

framing, 336

leased-line with PPP

authentication, 342-343

configuring PPP, 343-344

configuring PPP CHAP, 344-346

configuring PPP PAP, 346-347

control protocols, 341

framing, 341

multilink. See *MLPPP*

PPP functions, 340

MetroE, 364

access links, 365

data usage, 373-375

E-LAN service, 368-372

E-Line service, 367-371

E-Tree service, 369-372

full mesh topology, 368

hub and spoke topology, 369

IEEE Ethernet standards, 366

Layer 3 design, 370-372

MEF, 366

partial mesh topology, 369

physical design, 365-366

Point-to-Point topology, 367-368

services, 366

MPLS, 375-377

access links, 378

Layer 3 design, 377

MPLS VPNs, 379-382

QoS, 378-379

VPNs, 376

private

public cloud access, 746-749

public cloud branch office connections, 751

types, 362

public cloud connections

Internet as, 745-746

private WANs, 746-749

service providers (SPs), 362

wireless, 392-393

WAN interface cards (WICs), 332

WC masks. *See* wildcard masks

websites

APIC-EM Analysis tool released code, 777

APIC-EM labs, 777

ARIN, 174

BGP routing table analysis reports, 303

CCNA (ICND2) Config Labs, 796

CCNA Routing and Switching ICND2 Official Cert Guide, 777

Cisco

ACI, 774

APIC-EM pages, 777

DevNet, 777

Feature Navigator, 531

Prime management products, 695

Eclipse IDE, 744

ETSI, 754

Google App Engine PaaS, 744

IANA, 174

ICMPv6 parameters, 669

IPv6 multicast address space registry, 682

ICMPv6 packets, 669

Jenkins continuous integration and automation tool, 744

MEF, 366

OpenDaylight SDN controller, 771

OpenFlow, 768

Pearson Network Simulator (the Sim), 796

Wendell Odom's SDN Skills, 777

Wireshark network analyzer, 718

weighting, 505

Wendell Odom's SDN Skills blog, 777

WICs (WAN interface cards), 332

wildcard_mask parameter (network command), 198

wildcard masks

binary, 447

decimal, 446-447

EIGRP configuration, 248-249

finding, 448

OSPF single-area configuration, 199

wireless Internet, 393

wireless WANs, 392-393

Wireshark network analyzer, 718

workflow (virtualized data center), 737-738

working interfaces, 49

write views (SNMPv3 groups), 706