

CCNA 200-301

Hands-on Mastery with Packet Tracer



ciscopress.com

ANTHONY SEQUEIRA, CCIE® NO. 15626
RONALD WONG

FREE SAMPLE CHAPTER |



CCNA 200-301 Hands-on Mastery with Packet Tracer

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, Key Term flash card application, and Packet Tracer lab files!

To access the companion website, simply follow these steps:

1. Go to www.ciscopress.com/register.
2. Enter the **print book ISBN: 9780135313091**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at PearsonTestPrep.com. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to ciscopress.com/support.

This page intentionally left blank

CCNA 200-301 Hands-on Mastery with Packet Tracer

Anthony Sequeira, CCIE No. 15626

Ronald Wong

Cisco Press

Hoboken, New Jersey

CCNA 200-301 Hands-on Mastery with Packet Tracer

Anthony Sequeira; Ronald Wong

Copyright© 2025 Pearson Education, Inc.

Published by:
Cisco Press

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

\$PrintCode

Library of Congress Control Number: 2024945096

ISBN-13: 978-0-13-531309-1

ISBN-10: 0-13-531309-0

Warning and Disclaimer

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 provided is on an “as is” basis. The author and the publisher 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.

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.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose all such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

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.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

GM K12, Early Career and Professional Learning:	Copy Editor: Kitty Wilson
Soo Kang	Technical Editor: Wes Bryan
Alliances Manager, Cisco Press: Caroline Antonio	Editorial Assistant: Cindy Teeters
Director, ITP Product Management: Brett Bartow	Designer: Chuti Prasertsith
Managing Editor: Sandra Schroeder	Composition: codeMantra
Development Editor: Chris Zahn	Indexer: Timothy Wright
Senior Project Editor: Mandie Frank	Proofreader: Donna E. Mulder



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)

About the Authors

Anthony Sequeira (CCIE No. 15626) began his IT career in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion: teaching and writing about Microsoft and Cisco technologies. Anthony has lectured to massive audiences around the world while working for Mastering Computers. He has never been happier in his career than he is now as a senior technical instructor at ACI Learning. ACI is a leader in audit, cybersecurity, and IT pro training in self-paced and instructor-led formats. Follow Anthony today on X @compsolv or Facebook at facebook.com/compsolv.

Ronald Wong is the Director of Content Development for ACI Learning. He leads teams that are responsible for developing learning content for ACI. They develop courseware, labs, assessments, and ITPRO training. Previously Ronald has led Cisco, Microsoft Windows, CompTIA, and IT security training for the U.S. Army 7th SFG, the U.S. Air Force Special Operations Group, and the DoD at Ft. Lee. Most recently, Ronald was an Edutainer at ACI Learning and loved it. He takes a special interest in Networking Technology, especially Cisco, and tries his best to work as a good generalist in the IT field.

About the Technical Reviewer

Wesley Bryan, with nearly 15 years of experience as a technical instructor, specializes in CompTIA and Microsoft training. He began his journey as an IT student and discovered his passion for helping others launch their IT careers through certification and skills training. Wesley has served as a member of the Board of Directors for the North Florida Association of IT Professionals and participated in Instructor Advisory Boards. He is currently a technical instructor and subject matter expert for ACI Learning. Follow Wesley on Facebook via facebook.com/Wes.ITProTV, YouTube: youtube.com/@wsbryan1, and LinkedIn: linkedin.com/in/wesleyabryan.

Dedications

This book is dedicated to the countless CCNA students I have enjoyed helping over the decades I have worked in this industry. Keep up the inspired work!

—Anthony

To my family, friends, and co-workers, who somewhat pretended to be interested every time I talked about this book I was co-writing. Thanks for faking it so well! Someone owes me 50 bucks!

—Ronald

Acknowledgments

Thanks so much to Brett Bartow of Pearson for sharing our vision for this text. Also, huge thanks to Wes Bryan who meticulously edited every technical detail of this text.

Contents at a Glance

Introduction xxii

Part I Packet Tracer Fundamentals 1

Chapter 1 Introducing Packet Tracer 3

Chapter 2 Building Your First Simulation 15

Chapter 3 Customizing Packet Tracer 23

Part II Network Fundamentals 31

Chapter 4 Cisco IOS Basics 33

Chapter 5 Physical Interfaces and Cabling Types 47

Chapter 6 Configure and Verify IPv4 Addressing and Subnetting 61

Chapter 7 Configure IPv6 83

Chapter 8 Describe Wireless Principles 101

Chapter 9 Configure Switching Basics 107

Part III Network Access 117

Chapter 10 Configure and Verify VLANs and Interswitch Connectivity 119

Chapter 11 Configure and Verify Layer 2 Discovery Protocols 143

Chapter 12 Configure Rapid PVST+ Spanning Tree Protocol 151

Chapter 13 Compare Cisco Wireless Architectures and AP Modes 165

Part IV IP Connectivity 173

Chapter 14 Interpret the Components of a Routing Table 175

Chapter 15 Configure and Verify IPv4 and IPv6 Static Routing 189

Chapter 16 Configure and Verify Single Area OSPFv2 197

Part V IP Services 207

Chapter 17 Configure and Verify Inside Source NAT 209

Chapter 18 Configure and Verify NTP 221

Chapter 19 Configure DNS and DHCP 229

Chapter 20 Configure Other Networking Services 247

Part VI Security Fundamentals 261

Chapter 21 Configure Device Access Control 263

Chapter 22 Configure and Verify Access Control Lists 279

Chapter 23 Configure Layer 2 Security Features 293

Chapter 24 Configure Wireless Security Protocols 305

Part VII Appendices 311

Appendix A Other CCNA Topics 313

Appendix B Practice Exams 379

Glossary 429

Index 449

Reader Services

Register your copy of *CCNA 200-301 Hands-on Mastery with Packet Tracer* at www.ciscopress.com/title/ISBN for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780135313091 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

Contents

	Introduction	xxii
Part I	Packet Tracer Fundamentals	1
Chapter 1	Introducing Packet Tracer	3
	Accessing and Installing Cisco Packet Tracer	4
	Exploring Packet Tracer	9
	Chapter Review	13
Chapter 2	Building Your First Simulation	15
	Building the Lab Topology	15
	Lab 2.1: Building a Sample Lab	16
	Configuring and Verifying IP Reachability	19
	Lab 2.2: Configuring IP Reachability	19
	Chapter Review	22
Chapter 3	Customizing Packet Tracer	23
	Customizing Packet Tracer	23
	Lab 3.1: Customizing Packet Tracer	23
	Customizing Your First Simulation	27
	Lab 3.2: Customizing Your First Simulation	27
	Chapter Review	30
Part II	Network Fundamentals	31
Chapter 4	Cisco IOS Basics	33
	Chapter Pretest	34
	Answers	34
	The Cisco IOS CLI	35
	Lab 4.1: The Cisco IOS CLI	37
	Topic Quiz	38
	Topic Quiz Answers	39
	Configuring Cisco IOS	40
	Lab 4.2: Configuring Cisco IOS	42
	Topic Quiz	43
	Topic Quiz Answers	44
	Lab 4.3: Chapter Review	44
	Review Questions	45
	Answers to Review Questions	46

Chapter 5 Physical Interfaces and Cabling Types 47

Chapter Pretest	48
Answers	48
Single-Mode Fiber, Multimode Fiber, and Copper	49
Multimode Versus Single-Mode Fiber	50
Ethernet Shared Media Versus Point-to-Point	50
Power over Ethernet (PoE)	50
Serial Connections	51
Topic Quiz	52
Topic Quiz Answers	52
Troubleshoot Interface and Cable Issues (Collisions, Errors, Duplex, Speed)	52
Lab 5.1: Working with Interfaces and Cable Types	56
Topic Quiz	57
Topic Quiz Answers	57
Lab 5.2: Chapter Review	57
Review Questions	58
Answers to Review Questions	60

Chapter 6 Configure and Verify IPv4 Addressing and Subnetting 61

Chapter Pretest	62
Answers	63
Configure, Verify, and Troubleshoot IPv4 Addressing and Subnetting	64
Lab 6.1: IPv4 Address Configuration and Verification	68
Topic Quiz	69
Topic Quiz Answers	71
Compare and Contrast IPv4 Address Types	71
Lab 6.2: IPv4 Address Types	72
Topic Quiz	73
Topic Quiz Answers	74
Describe the Need for Private IPv4 Addressing	74
Topic Quiz	75
Topic Quiz Answers	76
Verify IP Parameters for Client OS (Windows, macOS, Linux)	76
Lab 6.3: Verify IPv4 on a Client OS	77
Topic Quiz	78
Topic Quiz Answers	79

	Lab 6.4: Chapter Review	79
	Review Questions	80
	Answers to Review Questions	81
Chapter 7	Configure IPv6	83
	Chapter Pretest	84
	Answers	85
	Compare and Contrast IPv6 Address Types	85
	Topic Quiz	88
	Topic Quiz Answers	89
	Configure, Verify, and Troubleshoot IPv6 Addressing	89
	Lab 7.1: IPv6 Address Configuration and Verification	90
	Lab 7.2: IPv6 EUI-64 Address Configuration and Verification	92
	Topic Quiz	94
	Topic Quiz Answers	94
	Verify IPv6 Parameters for the Client OS (Windows, macOS, Linux)	95
	Lab 7.3: IPv6 on a Client OS	96
	Topic Quiz	97
	Topic Quiz Answers	97
	Lab 7.4: Chapter Review	97
	Review Questions	98
	Answers to Review Questions	99
Chapter 8	Describe Wireless Principles	101
	Chapter Pretest	101
	Answers	102
	Wireless Principles	102
	Topic Quiz	103
	Topic Quiz Answers	103
	Lab 8.1: Chapter Review	104
	Review Questions	104
	Answers to Review Questions	105
Chapter 9	Configure Switching Basics	107
	Chapter Pretest	108
	Answers	108
	Describe Switching Concepts	109
	Topic Quiz	111

	Topic Quiz Answers	112
	Interpret Ethernet Frame Format	113
	Topic Quiz	114
	Topic Quiz Answers	114
	Lab 9.1: Chapter Review	114
	Review Questions	115
	Answers to Review Questions	116
Part III	Network Access	117
Chapter 10	Configure and Verify VLANs and Interswitch Connectivity	119
	Chapter Pretest	120
	Answers	120
	Configure, Verify, and Troubleshoot VLANs (Normal Range) Spanning Multiple Switches	121
	Lab 10.1: Configuring VLANs	125
	Topic Quiz	126
	Topic Quiz Answers	127
	Configure, Verify, and Troubleshoot Interswitch Connectivity	128
	Lab 10.2: Configuring Interswitch Connectivity	130
	Topic Quiz	131
	Topic Quiz Answers	131
	Configure, Verify, and Troubleshoot (Layer 2/Layer 3) EtherChannel	132
	Lab 10.3: Configuring EtherChannel	137
	Topic Quiz	138
	Topic Quiz Answers	139
	Lab 10.4: Chapter Review	139
	Review Questions	140
	Answers to Review Questions	141
Chapter 11	Configure and Verify Layer 2 Discovery Protocols	143
	Chapter Pretest	143
	Answers	144
	Configure and Verify Cisco Discovery Protocol (CDP)	144
	Topic Quiz	145
	Topic Quiz Answers	145
	Configure and Verify Link Layer Discovery Protocol (LLDP)	145
	Topic Quiz	146
	Topic Quiz Answers	147

	Lab 11.1: Chapter Review	147
	Review Questions	148
	Answers to Review Questions	149
Chapter 12	Configure Rapid PVST+ Spanning Tree Protocol	151
	Chapter Pretest	152
	Answers	152
	Understand Rapid PVST+ Spanning Tree Protocol	152
	Topic Quiz	160
	Topic Quiz Answers	161
	Lab 12.1: Chapter Review	161
	Review Questions	162
	Answers to Review Questions	163
Chapter 13	Compare Cisco Wireless Architectures and AP Modes	165
	Chapter Pretest	166
	Answers	166
	Using Cisco Wireless Architectures and AP Modes	166
	Topic Quiz	169
	Topic Quiz Answers	170
	Lab 13.1: Chapter Review	170
	Review Questions	171
	Answers to Review Questions	171
Part IV	IP Connectivity	173
Chapter 14	Interpret the Components of a Routing Table	175
	Chapter Pretest	176
	Answers	176
	Describe Routing Concepts	177
	Topic Quiz	178
	Topic Quiz Answers	178
	Interpret the Components of a Routing Table	179
	Topic Quiz	181
	Topic Quiz Answers	182
	Lab 14.1: Interpret a Routing Table	182
	Describe How a Routing Table Is Populated by Different Routing Information Sources	183
	Topic Quiz	184
	Topic Quiz Answers	185

Lab 14.2: Chapter Review 185
Review Questions 186
Answers to Review Questions 187

Chapter 15 Configure and Verify IPv4 and IPv6 Static Routing 189

Chapter Pretest 190
Answers 190
Configure, Verify, and Troubleshoot IPv4 and IPv6 Static Routing 190
Lab 15.1: IPv4 and IPv6 Static Routes 192
 Topic Quiz 193
 Topic Quiz Answers 194
Lab 15.2: Chapter Review 194
Review Questions 195
Answers to Review Questions 196

Chapter 16 Configure and Verify Single Area OSPFv2 197

Chapter Pretest 198
Answers 198
Configure, Verify, and Troubleshoot Single Area OSPFv2 for IPv4 198
Lab 16.1: OSPFv2 203
 Topic Quiz 203
 Topic Quiz Answers 204
Lab 16.2: Chapter Review 204
Review Questions 205
Answers to Review Questions 206

Part V IP Services 207

Chapter 17 Configure and Verify Inside Source NAT 209

Chapter Pretest 210
Answers 211
Configure, Verify, and Troubleshoot Inside Source NAT 211
Lab 17.1: NAT 216
 Topic Quiz 217
 Topic Quiz Answers 217
Lab 17.2: Chapter Review 217
Review Questions 218
Answers to Review Questions 219

Chapter 18	Configure and Verify NTP	221
	Chapter Pretest	222
	Answers	222
	Configure and Verify NTP Operating in Client/Server Mode	222
	Lab 18.1: NTP	224
	Topic Quiz	225
	Topic Quiz Answers	226
	Lab 18.2: Chapter Review	226
	Review Questions	227
	Answers to Review Questions	228
Chapter 19	Configure DNS and DHCP	229
	Chapter Pretest	230
	Answers	230
	Describe DNS Lookup Operation	231
	Topic Quiz	232
	Topic Quiz Answers	232
	Troubleshoot Client Connectivity Issues Involving DNS	233
	Topic Quiz	236
	Topic Quiz Answers	236
	Configure and Verify DHCP on a Router	236
	Lab 19.1: Configuring DHCP	240
	Topic Quiz	240
	Topic Quiz Answers	241
	Troubleshoot Client and Router-Based DHCP Connectivity Issues	241
	Topic Quiz	242
	Topic Quiz Answers	244
	Lab 19.2: Chapter Review	244
	Review Questions	245
	Answers to Review Questions	245
Chapter 20	Configure Other Networking Services	247
	Chapter Pretest	248
	Answers	248
	Describe the Use of Syslog and SNMP Features	249
	Lab 20.1: Configuring Syslog	252
	Topic Quiz	253
	Topic Quiz Answers	253

Explain the Forwarding Per-Hop Behavior (PHB) for QoS 253

Topic Quiz 255

Topic Quiz Answers 255

Using SSH and FTP/TFTP in a Network 256

Lab 20.2: Configuring SSH 256

Topic Quiz 257

Topic Quiz Answers 258

Lab 20.3: Chapter Review 258

Review Questions 259

Answers to Review Questions 260

Part VI Security Fundamentals 261

Chapter 21 Configure Device Access Control 263

Chapter Pretest 264

Answers 266

Configuring Device Access Controls 266

Lab 21.1: Configuring Device Access Controls 274

Topic Quiz 274

Topic Quiz Answers 275

Lab 21.2: Chapter Review 276

Review Questions 277

Answers to Review Questions 278

Chapter 22 Configure and Verify Access Control Lists 279

Chapter Pretest 280

Answers 283

Configure, Verify, and Troubleshoot IPv4 Standard Numbered and Named
Access Lists for Routed Interfaces 283

Lab 22.1: Configuring Access Control Lists 287

Topic Quiz 288

Topic Quiz Answers 289

Lab 22.2: Chapter Review 289

Review Questions 290

Answers to Review Questions 291

Chapter 23 Configure Layer 2 Security Features 293

Chapter Pretest 294

Answers 294

Configure Layer 2 Security Features 294

Lab 23.1: Configuring Layer 2 Security Features	299
Topic Quiz	300
Topic Quiz Answers	301
Lab 23.2: Chapter Review	301
Review Questions	302
Answers to Review Questions	303
Chapter 24 Configure Wireless Security Protocols	305
Chapter Pretest	306
Answers	306
Describe WPA, WPA2, and WPA3	306
Lab 24.1: Configuring Wireless Security	307
Topic Quiz	308
Topic Quiz Answers	309
Lab 24.2: Chapter Review	309
Review Questions	310
Answers to Review Questions	310
Part VII Appendices	311
Appendix A Other CCNA Topics	313
Appendix B Practice Exams	379
Glossary	429
Index	449

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.

Preface

Why is this book so valuable? Why is it an excellent resource to use prior to taking the CCNA 200-301 exam? Let us outline it for you here:

- This book balances the two potential areas of expertise you need for each exam topic. You either need to focus on just the theory of a technology or you need to be able to demonstrate a comprehensive understanding of configuration, verification, and troubleshooting in addition to the theory. You can trust this text to guide you through the precise knowledge you need, topic by topic.
- As alluded to above, this text is tightly focused on the exam. Whereas larger texts might provide background or peripheral information about a topic, this book is laser-focused on just those topics you need to comprehend for success in the exam environment. I certainly encourage the reading and study of larger works for those who require it.
- We have specialized in writing about and training candidates in all things CCNA since the inception of the certification in 1998. This book's technical reviewer also possesses vast knowledge in networking and cloud topics.
- We have taken the actual CCNA exam each and every revision since the certification's inception. We are therefore intimately familiar with the exam as well as with Cisco's testing techniques.
- This book is filled with valuable resources to assist you immediately in getting a passing score; these resources include quizzes, review questions, practice exams, and, of course, many hands-on labs using the superb Packet Tracer tool.

Introduction

Welcome to *CCNA 200-301 Hands-on Mastery with Packet Tracer*! This book covers the newly updated CCNA 200-301 certification exam. This new “one CCNA exam to rule them all” is more important than ever before in Cisco’s overall certification strategy. It covers the information you need to build a strong foundation for the varied CCNP certification tracks from Cisco Systems.

Whether this is your first or your fifteenth *CCNA textbook*, you’ll find information here that will ensure your success as you pursue knowledge, experience, and certification. This Introduction covers how this text can help you prepare for the CCNA exam.

This Introduction discusses the basics of the CCNA exam. Included are sections covering preparation, how to take an exam, a description of this book’s contents, how this book is organized, and, finally, author contact information.

Each chapter in this book contains practice questions. There are also two full-length Practice Exams at the end of the book. Practice Exams in this book should help you accurately assess the level of expertise you need in order to pass the test. Answers and explanations are included for all test questions. It is best to obtain a level of understanding equivalent to a consistent pass rate of at least 90% on the Review Questions and Practice Exams in this book before you take the real exam.

Let’s begin by looking at preparation for the exam.

How to Prepare for the Exam

This text follows the official exam objectives closely to help ensure your success. The official objectives from Cisco Systems can be found at <https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/ccna-200-301.html>.

As you examine the numerous exam topics now covered on the CCNA exam, resist the urge to panic! This book you are reading will provide you with the knowledge (and confidence) you need to succeed in taking this new CCNA exam. You just need to make sure you read it and follow the guidance it provides throughout your CCNA journey.

Practice Questions

This book is filled with practice questions to get you ready. Enjoy the following:

- **Chapter pretest questions at the beginning of each and every chapter:** These detailed, open-ended questions ensure that you really know the material. Some readers use these questions to “test out of” reading a particular section.
- **Topic-based quizzes ending each section:** These quizzes provide a chance to demonstrate your knowledge after completing a section.
- **Review questions ending each chapter:** These questions give you a final pass through the material covered in the chapter.

- **Two full practice exams:** The answer keys for the practice exams include explanations and tips for approaching each practice exam question.
- **Packet Tracer practice labs:** Every chapter challenges you with Packet Tracer practice labs. You simply download these labs from the book's companion website. These labs evaluate your progress and grade you when you complete each lab. Working through the practice labs will give you the knowledge and confidence you need in the actual exam.

Taking a Certification Exam

When you have prepared for the CCNA 200-301 exam, you must register with Cisco Systems to take the exam. The CCNA exam is given at Pearson VUE testing centers. Check the Pearson VUE website at www.pearsonvue.com to get specific details.

You can register for an exam online or by phone. After you register, you will receive a confirmation notice. Some areas may have limited testing centers available, so you should schedule your exam in advance to make sure you can get the specific date and time you would like.

Note You can now take the CCNA exam from your home or office. If you choose this option, be sure to review the requirements to ensure that you have no issues taking your exam in the privacy of your home or office.

Arriving at the Exam Location

As with any other examination, you should arrive at the testing center early. Be prepared! You need to bring two forms of identification (one with a picture). The testing center staff requires proof that you are who you say you are and that someone else is not taking the test for you. Arrive early because if you are late, you will be barred from entry and will not receive a refund for the cost of the exam.

Note You'll be spending a lot of time in the exam room. Plan on using the full two hours of time allotted for your exam and surveys. Policies differ from location to location regarding bathroom breaks, so check with the testing center before beginning the exam.

In the Testing Center

You will not be allowed to take into the examination room study materials or anything else that could raise suspicion that you're cheating. This includes practice test material, books, exam prep guides, and other test aids. The testing center will provide you with scratch paper and a pen or pencil—or possibly an erasable whiteboard.

After the Exam

Examination results are available immediately after the exam. If you pass the exam, you will simply receive a passing grade; your exact score will not be provided. Candidates who do not pass will receive a complete score breakdown by domain. This allows those individuals to see what areas they are weak in.

About This Book

The ideal reader for this text is someone seeking the CCNA certification. However, it should be noted that this book is very easily readable, and it rapidly presents facts. Therefore, this book is also extremely useful as a quick reference manual.

This book includes other helpful elements in addition to the actual logical, step-by-step learning progression of the chapters themselves. *There are plenty of quiz and review questions as well as plenty of labs to ensure that you are fully comprehending the material as you go.* This text also includes a very helpful Glossary to assist you.

Note Bulleted lists, numbered lists, tables, and graphics are also used where appropriate. A picture can paint a thousand words sometimes, and tables can help to associate different elements with each other visually.

Remember that you do not have to build your own Packet Tracer labs when using this book. We have built them for you. Be sure to visit the companion website for this text in order to download the Packet Tracer labs.

The Exam Blueprint

The table that follows outlines the CCNA exam domains and objectives and maps each objective to the chapter in the book that covers it in detail.

Exam Domain	Objective	Chapter in Book That Covers It
Network Fundamentals	Explain the role and function of network components	Appendix A
Network Fundamentals	Describe characteristics of network topology architectures	Appendix A
Network Fundamentals	Compare physical interface and cabling types	Chapter 5
Network Fundamentals	Identify interface and cable issues	Chapter 5
Network Fundamentals	Compare TCP to UDP	Appendix A
Network Fundamentals	Configure and verify IPv4 addressing and subnetting	Chapter 6

Exam Domain	Objective	Chapter in Book That Covers It
Network Fundamentals	Describe the need for private IPv4 addressing	Chapter 6
Network Fundamentals	Configure and verify IPv6 addressing and prefix	Chapter 7
Network Fundamentals	Describe IPv6 address types	Chapter 7
Network Fundamentals	Verify IP parameters for Client OS	Chapter 6
Network Fundamentals	Describe wireless principles	Chapter 8
Network Fundamentals	Explain virtualization fundamentals	Appendix A
Network Fundamentals	Describe switching concepts	Chapter 9
Network Access	Configure and verify VLANs spanning multiple switches	Chapter 10
Network Access	Configure and verify interswitch connectivity	Chapter 10
Network Access	Configure and verify Layer 2 discovery protocols	Chapter 11
Network Access	Configure and verify EtherChannel	Chapter 10
Network Access	Interpret basic operations of Rapid PVST+ Spanning Tree Protocol	Chapter 12
Network Access	Describe Cisco Wireless Architectures and AP modes	Chapter 13
Network Access	Describe physical infrastructure connections of WLAN components	Chapter 13
Network Access	Describe network device management access connections	Appendix A
Network Access	Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings	Appendix A
IP Connectivity	Interpret the components of a routing table	Chapter 14
IP Connectivity	Determine how a router makes a forwarding decision by default	Chapter 14
IP Connectivity	Configure and verify IPv4 and IPv6 static routing	Chapter 15
IP Connectivity	Configure and verify single area OSPFv2	Chapter 16

Exam Domain	Objective	Chapter in Book That Covers It
IP Connectivity	Describe the purpose, functions, and concepts of first hop redundancy protocols	Appendix A
IP Services	Configure and verify inside source NAT using static and pools	Chapter 17
IP Services	Configure and verify NTP operating in a client and server mode	Chapter 18
IP Services	Explain the role of DHCP and DNS within the network	Chapter 19
IP Services	Explain the function of SNMP in network operations	Chapter 20
IP Services	Describe the use of syslog features including facilities and levels	Chapter 20
IP Services	Configure and verify DHCP client and relay	Chapter 19
IP Services	Explain the forwarding per-hop behavior for QoS, such as classification, marking, queuing, congestion, policing, and shaping	Appendix A
IP Services	Configure network devices for remote access using SSH	Chapter 20
IP Services	Describe the capabilities and function of TFTP/FTP in the network	Chapter 20
Security Fundamentals	Describe key security concepts	Appendix A
Security Fundamentals	Describe security program elements	Appendix A
Security Fundamentals	Configure and verify device access control using local passwords	Chapter 21
Security Fundamentals	Describe security password policies elements, such as management, complexity, and password alternatives	Chapter 21
Security Fundamentals	Describe IPsec remote access and site-to-site VPNs	Appendix A
Security Fundamentals	Configure and verify access control lists	Chapter 22
Security Fundamentals	Configure and verify Layer 2 security features	Chapter 23
Security Fundamentals	Compare authentication, authorization, and accounting concepts	Appendix A

Exam Domain	Objective	Chapter in Book That Covers It
Security Fundamentals	Describe wireless security protocols	Chapter 24
Security fundamentals	Configure and verify WLAN within the GUI using WPA2 PSK	Chapter 24
Automation and Programmability	Explain how automation impacts network management	Appendix A
Automation and Programmability	Compare traditional networks with controller-based networking	Appendix A
Automation and Programmability	Describe controller-based, software-defined architecture	Appendix A
Automation and Programmability	Explain AI and machine learning in network operations	Appendix A
Automation and Programmability	Describe characteristics of REST-based APIs	Appendix A
Automation and Programmability	Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform	Appendix A
Automation and Programmability	Recognize components of JSON-encoded data	Appendix A

Other Book Elements

There are various important elements that are not part of the standard chapter format. These elements apply to the book as a whole.

- **Practice Exams:** In addition to including exam-preparation questions at the end of each chapter, this book provides two full Practice Exams.
- **Answers and explanations for practice exams:** An Answer Key follows each practice exam, providing answers to and explanations for the questions in the exams.
- **Glossary:** The Glossary defines important terms used in this book.
- **Companion website:** The companion website for this book allows you to access several digital assets that come with your book:
 - Pearson Test Prep software (both online and Windows desktop versions)
 - Key Terms Flash Cards application
 - A PDF version of the Command Reference
- The Packet Tracer Hands-On Labs

How to Access the Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials, as well as additional bonus content. Be sure to check the box indicating that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

- Step 1.** Go to www.ciscopress.com/register and log in or create a new account.
- Step 2.** Enter the ISBN: 9780135313091.
- Step 3.** Answer the challenge question as proof of purchase.
- Step 4.** Click the **Access Bonus Content** link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps above, please visit www.ciscopress.com/support. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software, containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions below.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- You can get your access code by registering the print ISBN (9780135313091) on ciscopress.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. After you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.

Note After you register your book, your code can always be found in your account on the Registered Products tab.

Once you have the access code, to find instructions about both the Pearson Test Prep web app and the desktop app, follow these steps:

- Step 1.** Open this book’s companion website, as shown earlier in this Introduction, under the heading, “How to Access the Companion Website.”
- Step 2.** Click the **Practice Test Software** button.
- Step 3.** Follow the instructions listed there for both installing the desktop app and using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsonstestprep.com, log in using the same credentials used to register your book, and register this book’s practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters; then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

Packet Tracer Hands-On Labs

Remember, the Packet Tracer labs are available for download from the companion website for this book.

If you do not have Packet Tracer (or if you have an older version that does not work with our files), be sure to register and download the latest free version from Cisco Networking Academy (<https://www.netacad.com>). As of this writing, Packet Tracer is available at <https://skillsforall.com>. Chapter 1 of this text walks you through the download and installation of this powerful network simulator.

Once you have Packet Tracer installed, you can simply double-click one of the PKA files to launch the topology and preexisting configurations in your version of Packet Tracer.

Contacting the Authors

Hopefully, this book provides you with the tools you need to pass the CCNA exam. Feedback is appreciated. You can contact the authors at ptracerbook@ajsnetworking.com.

Thank you for selecting our book; we have worked hard to apply the same concepts in this book that we have used in the hundreds of training classes we have taught. Spend your study time wisely and you, too, can become a CCNA. Good luck with the exam, although if you carefully work through this text, you will certainly minimize the amount of luck required!

Credits

Figures 6-4 and 19.1 - © Microsoft 2024

Cover: [simonkr/E+/Getty Images](#)

This page intentionally left blank

Configure and Verify Single Area OSPFv2

This chapter covers the following official CCNA 200-301 exam topic:

- Configure, verify, and troubleshoot single area OSPFv2 for IPv4

This chapter ensures that you understand OSPFv2 for the CCNA 200-301 exam from Cisco Systems. It is wonderful to see Cisco Systems finally bidding farewell to RIP when it comes to dynamic routing protocol coverage in the CCNA exam. Instead, the focus now is on a very scalable, exciting, and popular modern routing protocol option: OSPF version 2. This is the OSPF version designed for IPv4.

This chapter covers the following essential terms and components:

- OSPFv2
- **network** command
- Process ID
- Router ID
- Designated router (DR)
- Backup designated router (BDR)
- Point-to-point network type
- Broadcast network type
- Point-to-multipoint network type
- Non-broadcast network type
- Point-to-multipoint non-broadcast network type

Chapter Pretest

1. What aspect of OSPF makes the protocol hierarchical and permits the creation of very scalable networks?

2. What single OSPF router configuration command allows the assignment of OSPF area 0 to all interfaces in the range 10.0.0.0 to 10.255.255.255?

Answers

1. OSPF areas
2. `network 10.0.0.0 0.255.255.255 area 0`

Configure, Verify, and Troubleshoot Single Area OSPFv2 for IPv4

Open Shortest Path First (OSPF) is a beloved link-state routing protocol that is extremely configurable and scalable. It uses *areas* to reduce the size of convergence domains in the topology and ensure that scalability can be maintained. Remember that a convergence domain describes the set of routers that need to update their routing information whenever there is a change within that set.

OSPF version 2 is the current IPv4-only version of OSPF. OSPF version 3 is a standard for routing either IPv4 or IPv6 or both IPv4 and IPv6 simultaneously.

Figure 16.1 shows a sample topology, and Example 16.1 shows the configuration of OSPF in a single area of this topology, using the `network` command.

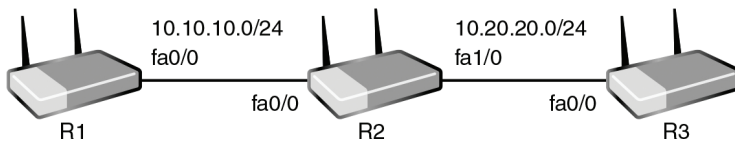


Figure 16.1 *Sample OSPF Topology*

Example 16.1 *Configuring Single Area OSPFv2 Using the network Command*

```
R1#
R1# configure terminal
R1(config)# router ospf 1
R1(config-router)# network 10.10.10.1 0.0.0.0 area 0
R1(config-router)# network 1.1.1.1 0.0.0.0 area 0
R1(config-router)# end
```

```

R1#
R2#
R2# configure terminal
R2(config)# router ospf 1
R2(config-router)# network 10.0.0.0 0.255.255.255 area 0
R2(config-router)# network 2.2.2.2 0.0.0.0 area 0
R2(config-router)# end
R2#
R3#
R3# configure terminal
R3(config)# router ospf 1
R3(config-router)# network 10.20.20.3 0.0.0.0 area 0
R3(config-router)# network 3.3.3.3 0.0.0.0 area 0
R3(config-router)# end
R3#

```

Notice the following details in the configuration in Example 16.1:

- **router ospf 1:** This command enters router configuration mode for OSPFv2 and sets a process ID of 1; this number is locally significant and does not need to match on the neighboring router.
- **network 10.10.10.1 0.0.0.0 area 0:** The **network** command sets the interface(s) that will run OSPF for this process; note that the wildcard mask 0.0.0.0 indicates that OSPF will run on the specific interface that has the IP address 10.10.10.1 (fa0/0); notice also that this interface participates in area 0, which is the backbone or core area for OSPF; all other areas must have contact with this backbone.

Example 16.2 shows how to easily verify OSPF.

Example 16.2 *Verifying Single Area OSPF*

```

R1#
R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
2.2.2.2 1 FULL/BDR 00:00:37 10.10.10.2 FastEthernet0/0
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route

```

```

Gateway of last resort is not set

    1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.1.1.0/24 is directly connected, Loopback0
L       1.1.1.1/32 is directly connected, Loopback0
    2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 10.10.10.2, 00:32:13, FastEthernet0/0
    3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/3] via 10.10.10.2, 00:19:12, FastEthernet0/0
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.10.0/24 is directly connected, FastEthernet0/0
L       10.10.10.1/32 is directly connected, FastEthernet0/0
O       10.20.20.0/24 [110/2] via 10.10.10.2, 00:32:33, FastEthernet0/0
R1# ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max &#61; 20/52/64 ms
R1#

```

Example 16.2 includes the following commands:

- **show ip ospf neighbor:** This command permits you to verify that you have an OSPF adjacency with your neighbor(s).
- **show ip route:** This command permits you to see the OSPF learned route information.
- **ping 3.3.3.3:** This command tests for full reachability; notice in Example 16.2, the R1 device is pinging an OSPF learned route from R3.

Note Several parameters must match in order for an OSPF neighborhood to form:

- The area ID
- Authentication settings
- Hello and dead intervals
- Stub flag
- MTU size

The hello and dead intervals are manipulated in interface configuration mode with the following commands:

```

(config-if)# ip ospf hello-interval 10
(config-if)# ip ospf dead-interval 30

```

The values used here indicate seconds.

Example 16.3 demonstrates single area OSPF configuration without the use of the **network** command.

Example 16.3 *Configuring Single Area OSPF Without the Use of the network Command*

```
R1#
R1# configure terminal
R1(config)# interface fa0/0
R1(config-if)# ip ospf 1 area 0
R1(config-if)# interface lo0
R1(config-if)# ip ospf 1 area 0
R1(config-if)# end
R1#
R2#
R2# configure terminal
R2(config)# interface fa0/0
R2(config-if)# ip ospf 1 area 0
R2(config-if)# interface fal/0
R2(config-if)# ip ospf 1 area 0
R2(config-if)# interface loopback 0
R2(config-if)# ip ospf 1 area 0
R2(config-if)# end
R2#
R3#
R3# configure terminal
R3(config)# interface fa0/0
R3(config-if)# ip ospf 1 area 0
R3(config-if)# interface loopback 0
R3(config-if)# ip ospf 1 area 0
R3(config-if)# end
R3#
```

Notice how simple it is to configure OSPF under the appropriate interfaces. As you can see, you do not have to enter OSPF router configuration mode at all for a basic configuration.

If you examine the **show ip ospf neighbor** command closely, you will notice some very interesting details in the output. First, note that the neighbor ID is listed. In Example 16.2, the neighbor ID value is 2.2.2.2. This is actually the router ID value for the OSPF speaker. This value is very important for various functions in OSPF. In fact, the router ID can be used in the election process of the DR and BDR devices in certain types of OSPF network configurations. This concept is discussed later in this chapter.

You can manually set a router ID for an OSPF router by using the `router-id` command, or you can allow the router to self-assign this value. How does the router choose its own router ID? It follows this order:

1. Use the manually configured router ID (if you configured it).
2. Use the numerically highest IP address on a loopback interface.
3. Use the numerically highest IP address on a non-loopback interface.

The `show ip ospf neighbor` command also indicates the current state of the neighbor. If you examine the output shown in Example 16.2, you will notice the state listed as `FULL/BDR`.

OSPF uses the following states in its operation in order to build and maintain neighbor relationships:

- Down
- Attempt
- Init
- 2-Way
- Exstart
- Exchange
- Loading
- Full

If there is a problem with a configuration or the underlying network, you might run your neighbor verification command and learn that your OSPF routers are stuck in one of the states that was supposed to be a transition state from Down to Full. Obviously, such information can help you dramatically in your troubleshooting.

What about the `BDR` indication in the output in Example 16.2? This indicates that the peer router is fulfilling the role of the backup designated router (BDR). The designated router (DR) and the BDR are used in certain types of network configurations for OSPF. They try to make the operation of OSPF more efficient by reducing the number of advertisements that must be made when sharing network information. Here is a list of the network types that are possible in OSPF and whether each one uses a DR and BDR in the operations of the protocol:

- **Broadcast:** DR/BDR used
- **Non-broadcast:** DR/BDR used
- **Point-to-point:** No DR/BDR
- **Point-to-multipoint:** No DR/BDR
- **Point-to-multipoint non-broadcast:** No DR/BDR

Lab 16.1: OSPFv2

To complete this Hands-On Lab Practice Assignment, download the assigned Packet Tracer file from the book's companion website and perform the lab on your locally installed version of Packet Tracer. You will be following the instructions in the lab, and your performance will be evaluated.

In this lab, you will configure and verify OSPFv2 using the topology shown in Figure 16.2.

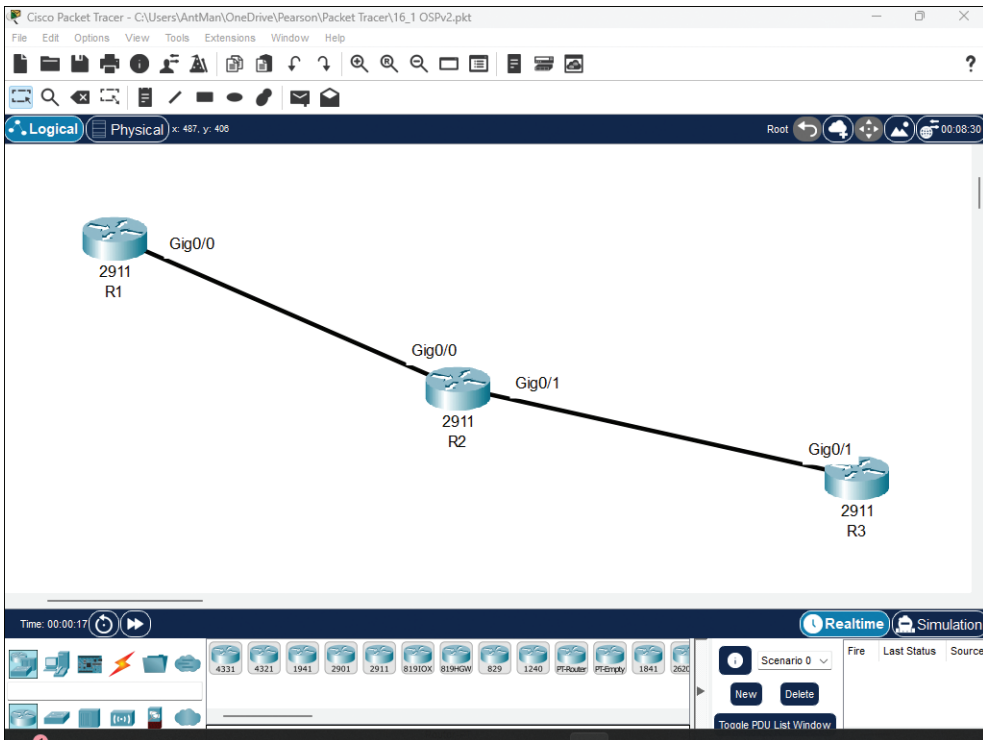


Figure 16.2 The OSPFv2 Lab

Topic Quiz

- Which statement about OSPFv2 is true?
 - The dead timers do not need to match between neighbors.
 - The hello timers do not need to match between neighbors.
 - The area ID must match between neighbors.
 - The `network` command must be used.

2. What command can you use to verify neighbors in OSPFv2?

- A. `show ospf neighbors`
- B. `show ip ospf neighbors`
- C. `show ospf database neighbors`
- D. `show ospf peers`

Topic Quiz Answers

1. C is correct. Area ID and hello and dead timers must match between neighbors.
2. B is correct. The `show ip ospf neighbors` command permits the verification of OSPF peerings.

Lab 16.2: Chapter Review

To complete this Hands-On Lab Practice Assignment, download the assigned Packet Tracer file from the book's companion website and perform the lab on your locally installed version of Packet Tracer. You will be following the instructions in the lab, and your performance will be evaluated.

In this lab, you will demonstrate the skills covered in this chapter using the topology shown in Figure 16.3.

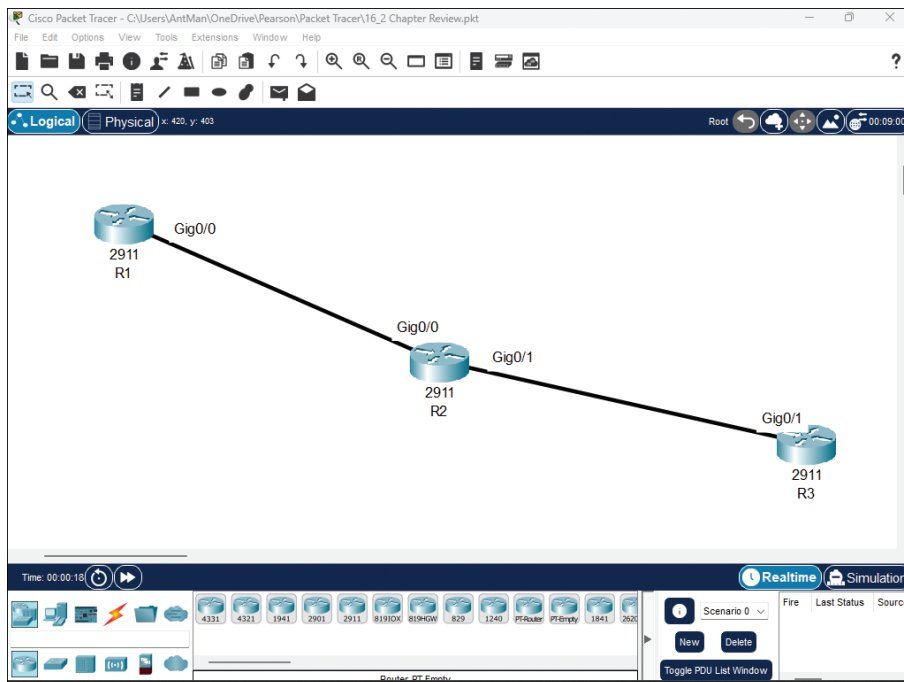


Figure 16.3 The OSPFv2 Chapter Review Lab

Review Questions

1. What command enters router configuration mode for OSPF version 2?
 - A. `router ospf 1`
 - B. `router ospf version 2`
 - C. `ospf router version 1`
 - D. `router ospf process 1 version 2`
2. You have configured OSPF on a router by using the command `network 10.10.0.0 0.0.255.255 area 0`. On which interface is OSPF running?
 - A. Gi0/0: 10.0.0.1 255.255.0.0
 - B. Gi0/1: 10.10.100.1 255.255.255.0
 - C. Gi0/2: 10.1.10.100 255.0.0.0
 - D. Gi0/3: 10.100.100.1 255.255.255.0
3. What does not have to match in order for an OSPF neighborship to form?
 - A. Area ID
 - B. MTU size
 - C. Hello and dead intervals
 - D. Use of the `network` command versus the `ip ospf` command
4. You have allowed a router to self-assign its router ID. What is the first option considered for the assignment on the device?
 - A. A random router ID assignment
 - B. The IP address on the highest-numbered interface name
 - C. The highest IP address on a physical interface
 - D. The highest IP address on a loopback interface
5. Which network type in OSPF features the use of a DR and a BDR?
 - A. Point-to-point
 - B. Broadcast
 - C. Point-to-multipoint
 - D. Point-to-multipoint non-broadcast

Answers to Review Questions

1. A is correct. The `router ospf 1` command enters router configuration mode for OSPF. It uses the local process ID 1.
2. B is correct. The `network 10.10.0.0 0.0.255.255 area 0` command ensures that OSPF runs on any interfaces that have IP addresses that have 10.10 in the first two octets. This is the Gi0/1 interface in this question.
3. D is correct. Neighborships can form in OSPF if one router uses the `network` command and the other uses the interface-level `ip ospf` command. Process IDs do not need to match between routers either.
4. D is correct. If you do not manually configure a router ID, the highest IP address on a loopback interface is used as the router ID. If there are no loopback interfaces, the router uses the highest IP address on a physical interface. If OSPF cannot find a configured IPv4 address, the OSPF process does not start.
5. B is correct. The DR and BDR devices are used in the broadcast and non-broadcast network types.

This page intentionally left blank

Index

Numerics

802.1Q, 128-130, 429
802.1X, 429

A

AAA (authentication, authorization, and accounting), 266, 353, 430
 local authentication
 configuring, 267
 verifying, 267
 RADIUS, 268
 TACACS+, 268
aaa new-model command, 267
access layer, 325
access points, 168–169, 315, 429
accessing
 CLI, 35
 Packet Tracer, 4–9
ACEs (access control entries), 283, 429
ACL (access control list), 283, 353
 configuring, 287–288
 extended, 283, 287, 435
 implicit deny entry, 284

 keywords, 284
 numbered, 284
 standard, 283
 assigning to an interface,
 285–286
 configuring, 285
 verifying, 284
 wildcards, 284
administrative distance, 181, 183, 429
adware, 350
AES (Advanced Encryption Standard),
 306
AI (artificial intelligence), 367, 429
 generative, 370–371
 machine learning, 371
 predictive, 371
alternate port, 429–430
Ansible, 372, 430
anycast, 87, 430
API (application programming
 interface), 364, 430
 RESTful, 363, 367, 369
 southbound, 363
application layer, 430
Application Virtualization Technology,
 430

area, OSPFv2, 198
 ARP (address resolution protocol), 429
 attenuation, 430
 authentication, local. *See also*
 password/s
 configuring, 267
 verifying, 267
 authoritative name servers, 231
 Auto MDI-X, 430
 autoconfiguration, IPv6, 87
 automation, 360, 361–362, 430
 AS (autonomous system), 430

B

baby giant frame, 54
 backup configuration, 430
 backup port, 430
 band, 102
 bandwidth, 430
 BDR (backup designated router), 202
 BE (best effort), 253
 BGP (Border Gateway Protocol), 431
 bidirectional NAT (Network Address Translation), 430–431
 bogon, 74
 boot field, 431
 BPDU (bridge protocol data unit), 153
 BPDU Filter, 160, 431
 BPDU Guard, 160
 bridge, 431
 broadcast transmission, 71–72, 431
 building, sample lab, 16–19

C

cabling, Ethernet

 crossover pin-out, 49
 fiber-optic, 50

 IEEE standards, 49
 Power over, 50–51
 straight-through pin-out, 49
 UTP (unshielded twisted pair), 49
 CAM (content-addressable memory), 432
 CAPWAP (Control and Provisioning of Wireless Access Points), 168–169, 432
 CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol), 306
 CDP (Cisco Discovery Protocol), 144, 431
 channel-group command, 133
 channels, 102, 431
 chassis aggregation, 431
 checksum, 431
 Chef, 431
 CIDR (classless interdomain routing), 432
 Cisco ACI (Application Centric Infrastructure), 326
 Cisco Catalyst 9800-L wireless controller, 166–167
 Cisco Catalyst Center, 319, 360–366, 431
 Cisco device
 passwords, 36
 privileged mode, 36
 Cisco DNA Center, 431–432
 Cisco IOS, 33
 CLI. *See* CLI
 command history buffer, 37
 configurations, 41–42
 configuring, 40–43
 help system, 36–37
 Cisco ISE (Identity Services Engine), 358
 Cisco switch, 10–13. *See also* switch/ing

- classful IPv4 addressing, 64–65, 432**
- classless addressing, 432**
- CLI, 37–38. *See also* command/s**
 - accessing, 35
 - Cisco switch, 10–13
 - login banner, configuring, 272–273
 - privileged mode, 36
 - user mode, 35
- client**
 - DHCP, configuring, 238
 - DNS configuration, 432
- client/server mode, NTP, 222–224**
- cloud, 330–332, 432**
 - hybrid, 331
 - IaaS (infrastructure as a service), 331
 - PaaS (platform as a service), 331
 - private, 331
 - public, 331
 - SaaS (software as a service), 331
 - XaaS (X as a service), 331
- collapsed core network design, 432**
- collision, 53, 432**
- command/s**
 - aaa new-model, 267
 - channel-group, 133
 - configure terminal, 20, 36, 123, 124, 129, 133, 190, 192, 212, 222, 237, 295, 297
 - copy running-config startup-config, 41–42
 - crypto key generate rsa, 272
 - debug, 40–41
 - default-router, 237
 - dns-server, 237
 - enable, 35
 - enable password, 270
 - enable secret, 270
 - help, 36–37
 - history buffer, 37
 - interface gigabitethernet, 20
 - interface range, 133
 - ip address dhcp, 238
 - ip arp inspection, 299
 - ip dhcp, 237
 - ip domain lookup, 236
 - ip domain-lookup, 236
 - ip domain-name, 236
 - ip name-server, 236
 - ip nat inside, 213
 - ip nat inside source, 215
 - ip nat inside source static, 213
 - ip nat outside, 213
 - ip ospf hello-interval, 200
 - ip ssh version 2, 272
 - ipconfig, 76
 - ipconfig /all, 95, 233–234
 - ipv6 enable, 92
 - logging buffered, 251
 - logging console, 251
 - logging host, 251
 - logging monitor warning, 251
 - login local, 267
 - network, 198–199, 238
 - no shutdown, 20
 - nslookup, 235
 - ntp master, 222–223
 - ntp server, 223
 - ntp server ntp-server-ip-address-or-dns-name, 223
 - option, 238
 - ping, 213, 235
 - router-id, 202
 - show, 40
 - show access-list, 286
 - show cdp, 145
 - show controllers, 51
 - show etherchannel, 134, 136–137
 - show interface, 125, 129–130

- show interfaces, 53, 54–56
- show ip dhcp binding, 238–239
- show ip dhcp conflict, 239
- show ip interface, 286
- show ip interface brief, 40, 239
- show ip nat translation, 213
- show ip ospf neighbor, 199–200, 202
- show ip route, 179, 191
- show ipv6 interface brief, 90
- show ipv6 route, 191–192
- show logging, 249–250
- show mac address-table, 110
- show ntp associations, 224
- show ntp status, 224
- show port-security, 295
- show port-security interface, 295–296, 297–298
- show run, 269
- show running-config, 13
- show spanning-tree, 154–156
- show vlan brief, 123, 124–125
- show vtp status, 122
- shutdown, 133
- transport input ssh, 272
- unicast-routing, 89
- username secret privilege, 267
- computer virus, 341**
- configuration register, 432**
- configurations**
 - Cisco IOS, 41–42
 - verifying, 42
- configure terminal command, 20, 36, 123, 124, 129, 133, 190, 192, 212, 222, 237, 295, 297**
- configuring. *See also* verifying**
 - ACL, 287–288
 - extended*, 287
 - standard*, 285
 - authentication, local, 267
 - Cisco IOS, 40–43
 - DHCP
 - client*, 238
 - server*, 237–238
 - dynamic inside source NAT, 214
 - EtherChannel, 137–138
 - inside source NAT, 212–213
 - interswitch connectivity, 130
 - IP reachability, 19–22
 - IPv4 addressing, 68–69
 - IPv6 addressing, 89, 90–92
 - login banner, 272–273
 - NTP client/server mode, 222–224
 - PAT (Port Address Translation), 215
 - port security, 294–295
 - RPVST+, 157–158
 - single area OSPF, 198–199, 201
 - SNMP, 252
 - Spanning Tree Protocol, PortFast, 159
 - SSH, 272
 - SSH on a device, 256–257
 - static port security, 296
 - Telnet, 271
 - VLAN, 123
 - interface*, 123–124
 - voice*, 124–125
- congestion avoidance, 255, 432**
- congestion management, 255**
- connectivity**
 - DHCP, troubleshooting, 241–242
 - DNS, troubleshooting, 233–236
- console, 432**
- container, 432**
- control plane, 433**
- controller-based SDN (software-defined network), 363**
- convergence, 254, 433**
- copy running-config startup-config command, 41–42**

core layer, 325
 CRC (cyclic redundancy check), 433
 creating
 EtherChannel, 133, 134–137
 VLAN on a switch, 122–123
 crossover pin-out, 49
 CRUD, 369, 433
 crypto key generate rsa command, 272
 cryptography, 358, 433
 CSMA/CA (carrier-sense multiple access with collision avoidance), 316, 431
 CSMA/CD (carrier-sense multiple access with collision detection), 50, 316, 431
 customizing
 Packet Tracer, 23–26
 simulation network, 27–30
 cut-through switching, 111

D

DAI (dynamic ARP inspection), 298–299, 434
 data access port, 433
 data exfiltration, 351
 data plane, 433
 DDoS (distributed denial-of-service) attack, 350–351
 debug command, 40–41
 de-encapsulation, 433
 default mask, 433
 default route, 433
 default routing, 433
 default VLAN, 123
 default-router command, 237
 defense in depth, 352
 delay, 433
 demarc, 433
 designated port, 153, 433

device/s. *See also* switch/ing; WLC (wireless LAN controller)
 adding to topology, 28–30
 DNA Center, 167
 hardening, 270, 272–273
 hub, 50
 SSH, configuring, 256–257
 switch, 50
 trust, 254, 433
 wireless, 102
 DHCP (Dynamic Host Configuration Protocol), 229, 236, 433–434
 client, configuring, 238
 connectivity, troubleshooting, 241–242
 relay agent, 239, 433–434
 server
 configuring, 237–238
 verifying, 238
 snooping, 298
 DiffServ, 254
 directed broadcast, 72
 distance vector protocol, 433
 distribution layer, 325
 DMVPN (Dynamic Multipoint VPN), 329, 358
 DNA Center, 167
 DNS (Domain Name System), 229, 433
 authoritative name servers, 231
 lookup operation, 231–232
 records, 232
 troubleshooting client connectivity issues, 233–236
 dns-server command, 237
 dotted-decimal notation, 433–434
 DR (designated router), 202
 duplex, 54
 full-, 53–54
 half-, 54
 dynamic inside source NAT, configuring, 214

dynamic port security, 434

dynamic route, 434

E

eBGP (External Border Gateway Protocol), 435

EGP (exterior gateway protocol), 435

EIGRP (Enhanced Interior Gateway Routing Protocol), 434

enable command, 35

enable password command, 270

enable secret command, 270

encapsulation, 434

endpoint, 316, 434

errdisable recovery, 434

escalation, 435

EtherChannel, 132, 435

 configuring, 137–138

 Layer 2, creating, 134–137

 static, creating, 133

Ethernet, 49

 cabling

crossover pin-out, 49

fiber-optic, 50

Power over, 50–51

UTP (unshielded twisted pair), 49

 frame, 435

baby giant, 54

format, 113

jumbo, 54

runts, 54

 IEEE standards, 49

 shared media environment, 50

 straight-through pin-out, 49

 switching, 435

EUI-64 address, 92–94

EXEC, 435

exploit, 352, 435

extended ACL (access control list), 283, 287

F

fault isolation, 435

FCS (frame check sequence), 436

FHRPs (First Hop Redundancy Protocols), 345–346, 435

 GLBP, 347

 HSRP, 346

 VRRP, 346

fiber-optic cable, 50

file system management, 435

firewall, 317–318, 435

flash, 435

floating static route, 192, 435

flow control, 435

fragment-free switching, 111

frame

 Ethernet

baby giant, 54

format, 113

jumbo, 54

runts, 54

 flooding, 110, 436

 keepalive, 438

 rewrite, 436

 switching, 110, 436

 tagging, 436

FTP (File Transfer Protocol), 256, 435

full-duplex, 53–54, 436

G

gateway of last resort, 181, 436

generative AI, 370–371, 436

GLBP (Gateway Load Balancing Protocol), 347
 global configuration mode, 436
 global unicast address, 86, 436
 GRE (generic routing encapsulation), 436

H

half-duplex, 54, 436
 header, 436
 IPv6, 85
 L2, 177–178
 help commands, 36–37
 hierarchical routing protocol, 436
 hop count, 222, 436
 host route, 436
 hostname, 436
 HSRP (Hot Standby Router Protocol), 346, 436
 HTTP, 369
 hubs, 50
 hybrid cloud, 331, 436
 hypervisor, 437

I

IaaS (infrastructure as a service), 331
 IANA (Internet Assigned Numbers Authority), 86
 iBGP (Interior Border Gateway Protocol), 437
 ICMP (Internet Control Message Protocol), 437
 IEEE standards, 437
 Ethernet, 49
 PoE (Power over Ethernet), 51
 wireless, 102
 implicit deny entry, 284, 437
 initial configuration dialog, 437

inside global, 437
 inside local, 437
 inside source NAT
 configuring, 212–213
 verifying, 213
 installation, Packet Tracer, 4–9
 interface gigabitethernet command, 20
 interface range command, 133
 interface/s, 18, 437
 assigning a standard ACL, 285–286
 CDP, enabling, 144
 LLDP, enabling, 146
 outgoing, 191
 router, 177
 speed, 54
 troubleshooting, 53, 54–56
 VLAN, configuring, 123–124
 interior routing protocol, 438
 inter-VLAN routing, 437
 IntServ, 254
 IOS (Internetwork Operating System).
 See Cisco IOS
 IOS recovery, 438
 IOS tool, 438
 IP (Internet Protocol), 437
 ip address dhcp command, 238
 ip arp inspection command, 299
 ip dhcp command, 237
 ip domain lookup command, 236
 ip domain-lookup command, 236
 ip domain-name command, 236
 ip name-server command, 236
 ip nat inside command, 213
 ip nat inside source command, 215
 ip nat inside source static command, 213
 ip nat outside command, 213
 ip ospf hello-interval command, 200
 IP reachability, configuring, 19–22

ip ssh version 2 command, 272
ipconfig /all command, 95, 233–234
ipconfig command, 76
IPS (intrusion prevention system), 438
IPsec, 358, 438
IPv4 address/ing, 56–57, 64. *See also* OSPFv2
 binary-to-decimal/decimal-to-binary conversion, 64
 broadcast, 71–72
 class, 64–65
 global unicast, 86
 multicast, 72
 need for, 74–75
 static routing, 190–191
 subnet mask, 65–68
 types, 72–73
 unicast transmission, 71
 verifying, 68–69
 verifying IP parameters for client OS, 76–78
IPv6 address/ing, 85, 438
 anycast, 87
 autoconfiguration, 87
 on a client OS, 96
 configuring, 89, 90–92
 EUI-64 address configuration and verification, 92–94
 format, 86
 header, 85
 prefix notation, 86
 SLAAC (stateless autoconfiguration), 92–93
 static routing, 191
 subnetting, 86
 types, 87
 verifying parameters for the client OS, 95–96
ipv6 enable command, 92
ISL (Inter-Switch Link), 128

J-K

JSON (JavaScript Object Notation), 374–375, 438
jumbo frame, 54

keepalive frame, 438
keywords, ACL, 284
KRACK (Key Reinstallation Attack), 307

L

L2 header rewrite, 177–178
lab
 building the topology, 15–19
 configuring access control lists, 287–288
 configuring device access control, 274
 configuring DHCP, 240
 configuring EtherChannel, 137–138
 configuring interswitch connectivity, 130
 configuring IP reachability, 19–22
 configuring Layer 2 security features, 299–300
 configuring VLANs, 125–126
 customizing Packet Tracer, 23–26
 customizing your first simulation, 27–30
 interpret a routing table, 182–184
 IPv4 address configuration and verification, 68–69
 IPv4 address types, 72–73
 IPv4 and IPv6 static routes, 192–193
 IPv6 address configuration and verification, 90–92
 IPv6 EUI-64 address configuration and verification, 92–94
 IPv6 on a client OS, 96
 NAT, 216

- NTP, 224–225
 - working with interfaces and cable types, 56–57
- LACP (Link Aggregation Control Protocol), 438
- LAG (link aggregation), 438
- laptop, adding to topology, 29
- Layer 2 EtherChannel, creating, 134–137
- Layer 2 security, 299–300
 - DAI (dynamic ARP inspection), 298–299
 - DHCP snooping, 298
 - port security
 - configuring*, 294–295
 - verifying*, 295–296
 - static port security
 - configuring*, 296
 - verifying*, 296–297
 - sticky MAC address learning, 297–298
- Layer 2/3 switch, 315
- licensing, 438
- link-local address, 87, 439
- link-state protocol, 439
- LLC (logical link control) sublayer, 439
- LLDP (Link Layer Discovery Protocol), 145–146, 438
 - enabling on an interface, 146
 - verifying, 146
- local authentication, 439
 - configuring, 267
 - verifying, 267
- local SPAN, 439
- logging, 439
- logging buffered command, 251
- logging console command, 251
- logging host command, 251
- logging monitor warning command, 251
- logical addressing, 439
- login banner, 272–273, 439

- login local command, 267
- Loop Guard, 159–160
- loopback address, 270, 439
- LSA (link-state advertisement), 439

M

- MAC address, 440
 - aging, 110
 - learning, 109, 439
 - sticky learning, 297–298
 - table, 110, 439
- machine learning, 371, 439
- malware, 350
- marking, 254, 439
- Martian packet, 74
- Maximum MAC address, 439
- MD5 Verify, 440
- mesh topology, 440
- messages, syslog, 250
- metric, 440
- Metro Ethernet, 328, 440
- mitigation, 440
- modified EUI-64, 87
- MPLS (Multiprotocol Label Switching), 328, 440
- multicast, 72, 87, 440
- multimode fiber, 50
- multipath routing protocol, 440
- multiplexing, 440

N

- named ACL (access control list), 440
- NAT (Network Address Translation), 74, 211–212, 434, 440
 - dynamic, configuring, 214
 - inside source
 - configuring*, 212–213

- verifying*, 213
- one-way, 212
- overloading. *See* PAT (Port Address Translation)
- static, 212
- troubleshooting, 216
- native VLAN, 440**
- network command, 198–199, 238**
- network/s. *See also* VPN (virtual private network); WAN (wide-area network)**
 - access layer, 325
 - cloaking, 103
 - converged, 254
 - core layer, 325
 - distribution layer, 325
 - endpoints, 316
 - full-duplex, 53–54
 - half-duplex, 54
 - loopback address, 270
 - OSI model, 337–339
 - on-premises, 322–330
 - server, 316
 - SOHO, 329
 - two-tier design, 326
 - two-tier spine-leaf topology, 326
 - virtual, 332
- next hop, 180, 441**
- NGFW (next-generation firewall), 317–318**
- NIC (network interface card), 440**
- no shutdown command, 20**
- northbound API, 441**
- nslookup command, 235**
- NTP (Network Time Protocol), 221, 222, 440**
 - client/server mode, 222–224
 - stratum, 222
- ntp master command, 222–223**
- ntp server command, 223**

- ntp server ntp-server-ip-address-or-dns-name command, 223**
- numbered ACL (access control list), 284, 441**
- NVRAM (nonvolatile random-access memory), 441**

O

- one-way NAT, 212**
- operating states, OSPFv2, 202**
- option command, 238**
- orchestration, 362**
- OSI model, 337–339, 441**
- OSPFv2, 197, 198, 441**
 - areas, 198
 - BDR (backup designated router), 202
 - DR (designated router), 202
 - neighborship, 200
 - operating states, 202
 - router ID, 201–202
 - single area
 - configuring*, 198–199, 201
 - verifying*, 199–200
- outgoing interface, 191**

P

- packet, Martian, 74**
- packet switching, 441**
- Packet Tracer, 3**
 - customizing, 23–26
 - installing, 4–9
 - sample topology, 9–12
- PAGP (Port Aggregation Protocol), 441**
- passive-interface, 441**
- password/s**
 - Cisco device, 36
 - policy, 268

- recovery, 441
- service password-encryption feature, 269–270
- PAT (Port Address Translation), 214, 441**
 - configuring, 215
 - verifying, 215–216
- on-path attack, 351**
- PDU (protocol data unit), 442**
- peerings, 441**
- peer-to-peer communication, 441**
- phishing, 351**
- ping command, 213, 235, 441**
- pin-out, Ethernet cabling, 49**
- PoE (Power over Ethernet), 50–51, 442**
- point-to-point link, 191**
- policing, 255, 441**
- policy**
 - password, 268
 - security, 353–354
- port LEDs, switch, 111**
- port security, 441**
 - configuring, 294–295
 - dynamic, 434
 - verifying, 295–296
- PortFast, 159, 442**
- PPPoE (Point-to-Point Protocol over Ethernet), 328**
- predictive AI, 371, 442**
- preemption, 442**
- on-premises, 322–330**
- presentation layer, 442**
- prioritization, 442**
- private cloud, 331, 442**
- private IPv4, 442**
- privileged mode, 36, 442**
- profile, WLC (wireless LAN controller), 167**
- programmability, 367, 369**
- protocol, 442**

- public cloud, 331, 442**
- puppet, 442**
- PVST+ (Per VLAN Spanning Tree Plus), 152, 441**

Q

- QoS (quality of service)**
 - BE (best effort), 253
 - congestion avoidance, 255
 - congestion management, 255
 - device trust, 254
 - DiffServ, 254
 - IntServ, 254
 - marking, 254
 - policing, 255
 - shaping, 254
 - WLC settings, 168

R

- RADIUS, 268**
- RAM (random-access memory), 442**
- ransomware, 351**
- records, DNS, 232**
- relay agent, DHCP, 239**
- remote access VPN (virtual private network), 356**
- RESTful API, 363, 369, 442–443**
- RFC 1918, 74, 75**
- RIP (Routing Information Protocol), 443**
- ROM (read-only memory), 442**
- ROM Monitor mode, 443**
- root bridge, 443**
- Root Guard, 159**
- root port, 153, 443**
- rootkit, 351**
- route aggregation, 443**

- routed protocol, 443
- router ID, OSPFv2, 201–202
- router-id command, 202
- router-on-a-stick, 443
- routing protocol, 443
- routing/router
 - gateway of last resort, 181
 - interface, 177
 - inter-VLAN, 437
 - L2 header rewrite, 177–178
 - static
 - IPv4*, 190–191
 - IPv6*, 191
 - verifying*, 191–192
 - syslog, 251
 - table, 179–181, 183, 443
- RPVST+ (Rapid Per VLAN Spanning Tree Plus)
 - configuring, 157–158
 - enhancements, 158–159
 - verifying, 158
- RSTP (Rapid Spanning Tree Protocol), 442
- running configuration, 443
- runts, 54

S

- SaaS (software as a service), 331
- sample lab, building, 15–19
- sample topology, 9–12
- saving, Cisco IOS configuration, 42
- SCP (Secure Copy Protocol), 443
- SDN (software-defined networking), 363, 444
 - architectures, 364
 - controller-based, 363, 364
- security. *See also* AAA; Layer 2 security
- ACL, 283. *See also* ACL (access control list)
 - extended*, 283
 - implicit deny entry*, 284
 - keywords*, 284
 - numbered*, 284
 - standard*, 283
 - wildcards*, 284
- attacks, 350–351
- defense in depth, 352
- exploit, 352
- loopback address, 270
- mitigation, 440
- password, 36
 - policy*, 268
 - service password-encryption feature*, 269–270
- policy, 353–354
- port
 - configuring*, 294–295
 - verifying*, 295–296
- vulnerability, 351
- wireless, 103
- WPA (Wi-Fi Protected Access)
 - AES (Advanced Encryption Standard)*, 306
 - CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)*, 306
 - KRACK (Key Reinstallation Attack)*, 307
 - TKIP (Temporal Key Integrity Protocol)*, 306
 - version 2*, 306, 307
 - version 3*, 307
- serial connections, 51
- server, 316
 - DHCP
 - configuring*, 237–238
 - verifying*, 238

- service password-encryption feature, 269–270, 271
- session layer, 443
- setup mode, 443
- severity levels, syslog, 250–251
- shaping, 254, 444
- shared media, 50
- show access-list command, 286
- show cdp command, 145
- show commands, 40
- show controllers command, 51
- show etherchannel command, 134, 136–137
- show interface command, 53, 54–56, 125, 129–130
- show ip dhcp binding command, 238–239
- show ip dhcp conflict command, 239
- show ip interface brief command, 40, 239
- show ip interface command, 286
- show ip nat translation command, 213
- show ip ospf neighbor command, 199–200, 202
- show ip route command, 179, 191
- show ipv6 interface brief command, 90
- show ipv6 route command, 191–192
- show logging command, 249–250
- show mac address-table command, 110
- show ntp associations command, 224
- show ntp status command, 224
- show port-security command, 295
- show port-security interface command, 295–296, 297–298
- show run command, 269
- show running-config command, 13
- show spanning-tree command, 154–156
- show vlan brief command, 123, 124–125
- show vtp status command, 122
- shutdown command, 133
- simulation network, customizing, 27–30
- single area OSPF
 - configuring, 198–199, 201
 - verifying, 199–200
- single-mode fiber, 50
- site-to-site VPN (virtual private network), 356–357
- SLA (service-level agreement), 438
- SLAAC (stateless autoconfiguration), 92–93
- sliding window, 444
- SMTP (Simple Mail Transfer Protocol), 444
- SNMP (Simple Network Management Protocol), 251, 444, 444
 - configuring, 252
 - security levels, 252
 - version 2, 251
 - version 3, 251–252
- socket, 444
- SOHO, 329
- source addressing, 444
- southbound API, 444
- Spanning Tree Protocol, 444
 - BPDU (bridge protocol data unit), 153
 - BPDU Filter, 160
 - BPDU Guard, 160
 - classic version, 153–154
 - configuring the priority value, 157
 - designated ports, 153
 - Loop Guard, 159–160
 - PortFast, 159
 - root bridge election, 153
 - Root Guard, 159
 - root port, 153
 - verifying, 154–157
 - verifying the root bridge, 157
- speed, interface, 54

- spyware, 350
- SQL injection attack, 351
- SSH (Secure Shell), 271, 443
 - configuring, 272
 - configuring on a device, 256–257
- SSID (service set identifier), 103, 443
- standard ACL (access control list), 283, 438
 - assigning to an interface, 285–286
 - configuring, 285
 - verifying, 284
- star topology, 444
- startup configuration, 444
- static EtherChannel, 444
 - creating, 133
- static NAT, 212, 444
- static port security, 444
 - configuring, 296
 - verifying, 296–297
- static routing, 192–193, 444
 - floating, 192
 - IPv4, 190–191
 - IPv6, 191
 - verifying, 191–192
- sticky MAC address learning, 297–298, 445
- store-and-forward switching, 111
- straight-through pin-out, 49
- stratum, 222, 445
- subinterface, 445
- subnet mask, 65–68, 445
- subnetting, 445
- SVI (switched virtual interface), 445
- switch/ing, 109, 445. *See also* VLAN (virtual local-area network)
 - connectivity, 130
 - cut-through, 111
 - default VTP status, 122
 - fragment-free, 111

- frame, 110
- frame flooding, 110
- L2/L3, 315
- MAC address
 - aging, 110
 - learning, 109
 - table, 110
- port LEDs, 111
- stacking, 445
- store-and-forward, 111
- switching, 50, 103
- syslog, 249, 445
 - default configuration, 249–250
 - message format, 250
 - router configuration, 251
 - severity levels, 250–251
 - timestamp information, 249

T

- TACACS+, 268, 445
- tags, WLC (wireless LAN controller), 167
- targeted broadcast, 72
- TCP (Transmission Control Protocol), 334, 445, 446
 - comparison with UDP, 340–342
 - three-way handshake, 338
- TCP/IP model, 337–339
- Telnet, 256, 445
 - configuring, 271
- terminal monitor, 445
- Terraform, 372–373, 445
- TFTP (Trivial File Transfer Protocol), 256, 446
- three-tier network design, 445
- three-way handshake, 338
- timestamp information, syslog, 249
- TKIP (Temporal Key Integrity Protocol), 306

TLS (Transport Layer Security), 356

topology

adding devices, 28–30

sample, 9–12

WAN, 327

traceroute, 445

trailer, 446

transport input ssh command, 272

transport layer, 446

Trojan horse, 350

troubleshooting, 446

DHCP connectivity, 241–242

DNS client connectivity, 233–236

interfaces, show interfaces command,
54–56

NAT (Network Address Translation),
216

trunk, 121–122, 128–130, 446

two-tier spine-leaf topology, 326, 429

U

**UDP (User Datagram Protocol), 334,
340–342, 446**

unicast transmission, 71, 87, 446

unicast-routing command, 89

unidirectional NAT, 446

unique local address, 87, 446

user mode, 35, 446

**username secret privilege command,
267**

UTP (unshielded twisted pair), 49

V

variable-length subnet masking, 68

verifying

configuration file, 42

DHCP server, 238

inside source NAT, 213

IPv4 address, 68–69

IPv4 parameters for client OS, 76–78

IPv6 parameters for the client OS,
95–96

LLDP, 146

local authentication, 267

PAT (Port Address Translation),
215–216

port security, 295–296

RPVST+, 158

single area OSPF, 199–200

Spanning Tree Protocol, 154–157

standard ACL, 284

static port security, 296–297

static routing, 191–192

VLAN, 123

virtual networking, 332

virus, 341

**VLAN (virtual local-area network), 121,
447**

802.1Q, 128–130

configuring and verifying, 123

creating on a switch, 122–123

default, 123

interface, configuring, 123–124

trunks, 121–122

voice, configuring, 124–125

**VLSM (variable-length subnet masking),
446**

VM (virtual machine), 447

voice port, 447

voice VLAN, configuring, 124–125

**VPN (virtual private network), 355,
358, 447**

cryptology, 358

dynamic multipoint, 358

IPsec, 358

remote access, 356

services, 357

site-to-site, 356–357

VRRP, 346
 VTP (VLAN Trunking Protocol),
 121–122, 447
 vty, 271, 447
 vulnerability, 351, 447

W

WAN (wide-area network), 327, 447
 DMVPN, 329
 Metro Ethernet, 328
 MPLS, 328
 PPPoE, 328
 topologies, 327
 well-known port, 447
 wildcard mask, 284, 447
 wireless technologies, 102. *See also*
 WLC (wireless LAN controller);
 WPA (Wi-Fi Protected Access)
 access points, 168–169, 315
 band, 102
 channels, 102
 IEEE standards, 102
 network cloaking, 103
 principles, 101–102
 security, 103
 SSID (service set identifier), 103

WLAN (wireless LAN), 168
 WLC (wireless LAN controller), 168,
 319–320, 447
 advanced properties, 168
 CAPWAP, 168–169
 Cisco Catalyst 9800-L wireless
 controller, 166–167
 profile, 167
 QoS settings, 168
 security settings, 168
 tags, 167
 worm attack, 350
 WPA (Wi-Fi Protected Access), 306,
 447
 AES (Advanced Encryption Standard),
 306
 CCMP (Counter Cipher Mode
 with Block Chaining Message
 Authentication Code Protocol), 306
 KRACK (Key Reinstallation Attack),
 307
 TKIP (Temporal Key Integrity
 Protocol), 306
 version 2, 306, 307
 version 3, 307

X-Y-Z

zero-day attack, 352