Enterprise Networking, Security, and Automation Labs and Study Guide (CCNAv7)

Instructor's Answer Key

Allan Johnson

Networking Academy

Cisco Press

221 River St.

Hoboken, NJ 07030 USA

Enterprise Networking, Security, and Automation Labs and Study Guide (CCNAv7)

Instructor's Answer Key

Published by
Cisco Press
221 River St.
Hoboken, NJ 07030 USA

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020906042

Student ISBNs:

ISBN-13: 978-0-13-663469-0
ISBN-10: 0-13-663469-9

Instructor ISBNs:

ISBN-13: 978-0-13-663471-3
ISBN-10: 0-13-663471-0

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Alliances Manager, Cisco Press
Arezou Gol

Senior Editor
James Manly

Managing Editor
Sandra Schroeder

Development Editor
Ellie Bru

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Technical Editor
Dave Holzinger

Editorial Assistant
Cindy Teeters

Designer
Chuti Prasertsith

Composition
codeMantra

Proofreader
Charlotte Kughen

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.netacad.com

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Switching, Routing, and Wireless Essentials (CCNAv7) course. 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.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

About the Contributing Author

Allan Johnson entered the academic world in 1999, after 10 years as a business owner/operator, to dedicate his efforts to his passion for teaching. He holds both an M.B.A. and an M.Ed. in training and development. He taught CCNA courses at the high school level for 7 years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as Curriculum Lead.

About the Technical Reviewer

Dave Holzinger has been a curriculum developer, project manager, author, and technical editor for Cisco Networking Academy in Phoenix since 2001. Dave works on the team that develops Cisco Networking Academy's online curricula, including CCNA, CCNP, and IT Essentials. He has been working with computer hardware and software since 1981. Dave has certifications from Cisco, BICSI, and CompTIA.

Contents at a Glance

Introduction xxviii

Chapter 1 Single-Area OSPFv2 Concepts 1

Chapter 2 Single-Area OSPFv2 Configuration 15

Chapter 3 Network Security Concepts 77

Chapter 4 ACL Concepts 123

Chapter 5 ACLs for IPv4 Configuration 135

Chapter 6 NAT for IPv4 201

Chapter 7 WAN Concepts 249

Chapter 8 VPN and IPsec Concepts 271

Chapter 9 QoS Concepts 289

Chapter 10 Network Management 305

Chapter 11 Network Design 399

Chapter 12 Network Troubleshooting 413

Chapter 13 Network Virtualization 449

Chapter 14 Network Automation 463

Contents

Introduction xxviii

Chapter 1 Single-Area OSPFv2 Concepts 1

Study Guide 2

OSPF Features and Characteristics 2

Components of OSPF 2

Link-State Operation 2

Single-Area and Multiarea OSPF 3

OSPFv3 3

Check Your Understanding—OSPF Features and Characteristics 4

OSPF Packets 5

Types of OSPF Packets 5

Link-State Updates 5

Hello Packet 6

Check Your Understanding—OSPF Packets 7

OSPF Operation 8

OSPF Operational States 8

The Need for a DR 11

LSA Flooding with a DR 12

Check Your Understanding—OSPF Operation 12

Labs and Activities 14

Chapter 2 Single-Area OSPFv2 Configuration 15

Study Guide 16

OSPF Router ID 16

OSPF Reference Topology 16

Router IDs 16

Router ID Order of Precedence 17

Configure a Loopback Interface as the Router ID 18

Explicitly Configure a Router ID 18

Modify the Router ID 18

Check Your Understanding—OSPF Router ID 18

Point-to-Point OSPF Networks 19

The network Command Syntax 19

The Wildcard Mask 20

Configure OSPF Using the network Command 20

Configure OSPF Using the ip ospf Command 20

Passive Interface 21

Configure Passive Interfaces 21

Packet Tracer Exercise 2-1: Point-to-Point Single-Area OSPFv2 Configuration 21

Multiaccess OSPF Networks 22
OSPF Designated Router 22
OSPF Multiaccess Reference Topology 22
Verify OSPF Multiaccess Router Roles 23
DR Failure and Recovery 24
Configure OSPF Priority 24
Modify Single-Area OSPFv2 25
Cisco OSPF Cost Metric 25
Adjust the Reference Bandwidth 25
OSPF Accumulates Cost 26
Manually Set OSPF Cost Value 27
Modify OSPFv2 Intervals 28
Default Route Propagation 28
Propagate and Verify a Default Route 28
Packet Tracer Exercise 2-2—Modify a Point-to-Point Single-Area OSPFv2 Configuration 29
Verify Single-Area OSPFv2 30
Verify OSPF Neighbors 30
Verify OSPF Protocol Settings 31
Verify OSPF Process Information 31
Verify OSPF Interface Settings 32
Labs and Activities 34
Command Reference 34
2.2.13 Packet Tracer—Point-to-Point Single-Area OSPFv2 Configuration (Instructor Version) 35
Addressing Table 35
Objectives 35
Background 35
Instructions 35
Part 1: Configure Router IDs 35
Part 2: Configure Networks for OSPF Routing 36
Part 3: Configure Passive Interfaces 38
Part 4: Verify OSPF Configuration 38
Answer Scripts 38
Router R1 38
Router R2 39
Router R3 39
2.3.11 Packet Tracer—Determine the DR and BDR (Instructor Version) 40
Addressing Table 40
Objectives 40
Scenario 40
Instructions 40

Part 1: Examine DR and BDR Changing Roles 40
Part 2: Modify OSPF Priority and Force Elections 43

2.4.11 Packet Tracer—Modify Single-Area OSPFv2 (Instructor Version) 44
Addressing Table 44
Objectives 44
Scenario 44
Instructions 44
Part 1: Modify OSPF Default Settings 44
Part 2: Verify Connectivity 46
Answer Scripts 46
Router R1 46
Router R2 46

2.5.3 Packet Tracer—Propagate a Default Route in OSPFv2 (Instructor Version) 47
Addressing Table 47
Objectives 47
Background 47
Instructions 47
Part 1: Propagate a Default Route 47
Part 2: Verify Connectivity 49
Answer Script 49
Router R2 49

2.6.6 Packet Tracer—Verify Single-Area OSPFv2 (Instructor Version) 50
Addressing Table 50
Objectives 50
Background / Scenario 50
Instructions 51
Part 1: Verify the Existing OSPFv2 Network Operation 51
Part 2: Add the New Branch Office LAN to the OSPFv2 Network 54

2.7.1 Packet Tracer—Single-Area OSPFv2 Configuration (Instructor Version) 55
Addressing Table 55
Objectives 55
Background 55
Instructions 56
Requirements 56
Answer Configurations 56
P2P-1 56
P2P-2 57
P2P-3 57
BC-1 57
BC-2 58
BC-3 58

2.7.2 Lab—Configure Single-Area OSPFv2 (Instructor Version) 59
Topology 59
Addressing Table 59
Objectives 59
Background / Scenario 59
Required Resources 60
Instructions 60
Part 1: Build the Network and Configure Basic Device Settings 60
Part 2: Configure and Verify Single-Area OSPFv2 for Basic Operation 62
Part 3: Optimize the Single-Area OSPFv2 Configuration 64
Router Interface Summary Table 66
Device Configs 67
Router R1 67
Router R2 69
Switch S1 71
Switch S2 74

Chapter 3 Network Security Concepts 77

Study Guide 78

Current State of Cybersecurity 78
Current State of Affairs 78
Vectors of Network Attacks 78
Data Loss 79
Check Your Understanding—Current State of Cybersecurity 80

Threat Actors 81
The Hacker 81
Evolution of Hackers 81
Check Your Understanding—Threat Actors 82

Threat Actor Tools 82
Video—Threat Actor Tools 83
Evolution of Security Tools 83
Attack Types 84
Check Your Understanding—Threat Actor Tools 84

Malware 85
Viruses and Trojan Horses 85
Other Types of Malware 86
Check Your Understanding—Malware 87

Common Network Attacks 89
Overview of Network Attacks 89
Video—Reconnaissance Attacks 89
Reconnaissance Attacks 89
Video—Access and Social Engineering Attacks 90
Access Attacks 90

Social Engineering Attacks 90
Video—Denial of Service Attacks 91
DoS and DDoS Attacks 91
Check Your Understanding—Common Network Attacks 92

IP Vulnerabilities and Threats 92
Video—Common IP and ICMP Attacks 93
IPv4 and IPv6 93
ICMP Attacks 93
Video—Amplification, Reflection, and Spoofing Attacks 94
Amplification and Reflection Attacks 94
Address Spoofing Attacks 94
Check Your Understanding—IP Vulnerabilities and Threats 95

TCP and UDP Vulnerabilities 96
TCP Segment Header 96
TCP Services 97
TCP Attacks 98
Check Your Understanding—TCP and UDP Vulnerabilities 99

IP Services 100
ARP Vulnerabilities 100
Video—ARP Spoofing 100
DNS Attacks 101
DHCP 101
DCHP Spoofing Attacks 102

Network Security Best Practices 102
Confidentiality, Integrity, and Availability (CIA) 102
The Defense-in-Depth Approach 102
IPS 103
Content Security Appliances 104
Check Your Understanding—Network Security Best Practices 105

Cryptography 106
Video—Cryptography 106
Securing Communications 106
Data Integrity 107
Origin Authentication 107
Data Confidentiality 108
Symmetric Encryption 108
Asymmetric Encryption 109
Diffie-Hellman 110
Check Your Understanding—Cryptography 111

Labs and Activities 112

3.5.7 Lab—Social Engineering (Instructor Version) 112
Objective 112

Resources 112
Instructions 112

3.8.8 Lab—Explore DNS Traffic (Instructor Version) 114

Objectives 114
Background / Scenario 114
Required Resources 114
Instructions 114
Reflection Question 121

Chapter 4 ACL Concepts 123

Study Guide 124

Purpose of ACLs 124

ACL Operation 124
Check Your Understanding—Purpose of ACLs 124

Wildcard Masks in ACLs 125

Wildcard Mask Overview 125
Wildcard Mask Types 126
Wildcard Mask Calculation 126
Wildcard Mask Keywords 127
Check Your Understanding—Wildcard Masks in ACLs 127

Guidelines for ACL Creation 128

Limited Number of ACLs per Interface 128
ACL Best Practices 129
Check Your Understanding—Guidelines for ACL Creation 129

Types of IPv4 ACLs 129

Standard and Extended ACLs 130
Numbered and Named ACLs 130
Standard and Extended ACL Placement 130
Check Your Understanding—Types of IPv4 ACLs 131

Labs and Activities 132

4.1.4 Packet Tracer—Access Control List Demonstration (Instructor Version) 132

Objectives 132
Background 132
Addressing Table 132
Instructions 133
Part 1: Verify Local Connectivity and Test Access Control List 133
Part 2: Remove the ACL and Repeat the Test 133

Chapter 5 ACLs for IPv4 Configuration 135

Study Guide 136

Configure Standard IPv4 ACLs 136

Create an ACL 136
Numbered Standard IPv4 ACLs 136
Apply a Standard IPv4 ACL 137
Named Standard IPv4 ACLs 137
Standard IPv4 ACL Scenarios 138

Modify IPv4 ACLs 139
Sequence Numbers Method 139

Secure VTY Ports with a Standard IPv4 ACL 140
The access-class Command 140
Secure VTP Access Example 140

Configure Extended IPv4 ACLs 140
Extended ACLs 141
Numbered Extended IPv4 ACLs 141
Numbered Extended ACL Configuration Scenarios 141
Evaluate Extended IPv4 ACL Statements 142
Extended ACL Quiz 144

Labs and Activities 146

Command Reference 146

5.1.8 Packet Tracer—Configure Numbered Standard IPv4 ACLs (Instructor Version) 147
Addressing Table 147
Objectives 147
Background / Scenario 147
Instructions 147
Part 1: Plan an ACL Implementation 147
Part 2: Configure, Apply, and Verify a Standard ACL 148
Answer Configurations 150
Router R2 150
Router R3 150

5.1.9 Packet Tracer—Configure Named Standard IPv4 ACLs (Instructor Version) 151
Addressing Table 151
Objectives 151
Background / Scenario 151
Instructions 151
Part 1: Configure and Apply a Named Standard ACL 151
Part 2: Verify the ACL Implementation 152
Answer Scripts 152
Router R1 152

5.2.7 Packet Tracer—Configure and Modify Standard IPv4 ACLs (Instructor Version) 153
Addressing Table 153
Objectives 153

Background / Scenario 153
Instructions 154
Part 1: Verify Connectivity 154
Part 2: Configure and Verify Standard Numbered and Named ACLs 154
Part 3: Modify a Standard ACL 159
Reflection Questions 161
Answer Scripts 161
Router R1 161
Router R3 162

5.4.12 Packet Tracer—Configure Extended ACLs—Scenario 1 (Instructor Version) 163

Addressing Table 163
Objectives 163
Background / Scenario 163
Instructions 163
Part 1: Configure, Apply, and Verify an Extended Numbered ACL 163
Part 2: Configure, Apply, and Verify an Extended Named ACL 166
Answer Script 167
Router R1 167

5.4.13 Packet Tracer—Configure Extended IPv4 ACLs—Scenario 2 (Instructor Version) 168

Addressing Table 168
Objectives 168
Background / Scenario 168
Instructions 168
Part 1: Configure a Named Extended ACL 168
Part 2: Apply and Verify the Extended ACL 170
Answer Configuration 171
Router RT1 171

5.5.1 Packet Tracer—IPv4 ACL Implementation Challenge (Instructor Version) 173

Addressing Table 173
Objectives 173
Background / Scenario 173
Instructions 174
Answer Scripts 176
Router HQ 176
Router Branch 176

5.5.2 Lab—Configure and Verify Extended IPv4 ACLs (Instructor Version) 177

Topology 177
Addressing Table 177
VLAN Table 177

Objectives 178
Background / Scenario 178
Required Resources 178
Instructions 178
Part 1: Build the Network and Configure Basic Device Settings 178
Part 2: Configure VLANs on the Switches 180
Part 3: Configure Trunking 182
Part 4: Configure Routing 183
Part 5: Configure Remote Access 184
Part 6: Verify Connectivity 185
Part 7: Configure and Verify Extended Access Control Lists 185
Device Configs 186
Router R1 186
Router R2 190
Switch S1 192
Switch S2 196

Chapter 6 NAT for IPv4 201

Study Guide 202

NAT Characteristics 202
IPv4 Private Address Space 202
NAT Terminology 202
Check Your Understanding—NAT Characteristics 203

Types of NAT 204
Static NAT 204
Dynamic NAT 204
Port Address Translation 204
NAT and PAT Comparison 204

NAT Advantages and Disadvantages 204
Check Your Understanding—NAT Advantages and Disadvantages 205

Static NAT 205
Configure Static NAT 206
Packet Tracer Exercise 6-1: Configure Static NAT 206

Dynamic NAT 207
Configure Dynamic NAT 207
Packet Tracer Exercise 6-2: Configure Dynamic NAT 208

PAT 209
Configure PAT 209

NAT64 213

Labs and Activities 214

Command Reference 214

6.2.7 Packet Tracer—Investigate NAT Operations (Instructor Version) 214
Addressing Table 214
Objectives 215
Scenario 215
Instructions 215
Part 1: Investigate NAT Operation Across the Intranet 215
Part 2: Investigate NAT Operation Across the Internet 216
Part 3: Conduct Further Investigations 217
6.4.5 Packet Tracer—Configure Static NAT (Instructor Version) 219
Objectives 219
Scenario 219
Instructions 219
Part 1: Test Access Without NAT 219
Part 2: Configure Static NAT 220
Part 3: Test Access with NAT 220
6.5.6 Packet Tracer—Configure Dynamic NAT (Instructor Version) 221
Objectives 221
Instructions 221
Part 1: Configure Dynamic NAT 221
Part 2: Verify NAT Implementation 222
Answer Script 222
Router R2 222
6.6.7 Packet Tracer—Configure PAT (Instructor Version) 223
Objectives 223
Part 1: Configure Dynamic NAT with Overload 223
Part 2: Verify Dynamic NAT with Overload Implementation 224
Part 3: Configure PAT Using an Interface 224
Part 4: Verify PAT Interface Implementation 225
Answer Configurations 225
Router R1 225
Router R2 226
6.8.1 Packet Tracer—Configure NAT for IPv4 (Instructor Version) 227
Addressing Table 227
Objectives 227
Background / Scenario 227
Instructions 227
Answer Configurations 228
Router R2 228
6.8.2 Lab—Configure NAT for IPv4 (Instructor Version) 229
Topology 229
Addressing Table 229
Objectives 229

Background / Scenario 229
Required Resources 230
Instructions 230
Part 1: Build the Network and Configure Basic Device Settings 230
Part 2: Configure and Verify NAT for IPv4 232
Part 3: Configure and Verify PAT for IPv4 234
Part 4: Configure and Verify Static NAT for IPv4 237
Router Interface Summary Table 238
Device Configs - Final 238
Router R1 238
Router R2 240
Switch S1 242
Switch S2 245

Chapter 7 WAN Concepts 249

Study Guide 250

Purpose of WANs 250

LANs and WANs 250
WAN Topologies 250
Evolving Networks 251
Check Your Understanding—Purpose of WANs 252

WAN Operations 253

WAN Standards 253
WAN Terminology and Devices 254
Check Your Understanding—WAN Operations 255

Traditional WAN Connectivity 256

Traditional WAN Connectivity Options 256
Leased Lines 257
Legacy Switched WAN Options 258
Check Your Understanding—Traditional WAN Connectivity 258

Modern WAN Connectivity 259

Modern WANs 259
Modern WAN Connectivity Options 260
Check Your Understanding—Modern WAN Connectivity 261

Internet-Based Connectivity 261

Internet-Based Connectivity Terminology 261

Labs and Activities 263

7.5.11 Lab—Research Broadband Internet Access Technologies (Instructor Version) 263

Objectives 263
Background / Scenario 263
Required Resources 263

Part 1: Investigate Broadband Distribution 263
Part 2: Research Broadband Access Options for Specific Scenarios 265
Reflection Question 266

7.6.1 Packet Tracer—WAN Concepts (Instructor Version) 267
Objectives 267
Background / Scenario 267
Instructions 267
Part 1: Investigate Consumer WAN Technologies for Home and Mobile Devices 267
Part 2: Explore Connectivity 270

Chapter 8 VPN and IPsec Concepts 271

Study Guide 272

VPN Technology 272
Virtual Private Networks 272
VPN Benefits 272
Site-to-Site and Remote-Access VPNs 273
Enterprise and Service Provider VPNs 273
Check Your Understanding—VPN Technology 274

Types of VPNs 275
Remote-Access VPNs 275
SSL and IPsec 276
Site-to-Site IPsec VPNs 276
GRE over IPsec 276
Dynamic Multipoint VPNs 277
IPsec Virtual Tunnel Interface 278
Service Provider MPLS VPNs 278
Check Your Understanding—Types of VPNs 278

IPsec 279
Video—IPsec Concepts 279
IPsec Technologies 279
IPsec Protocol Encapsulation 281
Confidentiality 281
Integrity 282
Authentication 283
Secure Key Exchange with Diffie-Hellman 283
Video—IPsec Transport and Tunnel Mode 284
Check Your Understanding—IPsec 284

Labs and Activities 287

Chapter 9 QoS Concepts 289

Study Guide 290

Network Transmission Quality 290

Video Tutorial—The Purpose of QoS 290
Network Transmission Quality Terminology 290
Check Your Understanding—Network Transmission Quality 291

Traffic Characteristics 292

Video Tutorial—Traffic Characteristics 292
Traffic Characteristics 292
Check Your Understanding—Traffic Characteristics 292

Queuing Algorithms 293

Video Tutorial—QoS Algorithms 293
Identify the Queuing Algorithm 293
Queuing Algorithm Characteristics 295
Check Your Understanding—Queuing Algorithms 296

QoS Models 297

Video Tutorial—QoS Models 297
QoS Model Characteristics 297
Check Your Understanding—QoS Models 298

QoS Implementation Techniques 299

Video Tutorial—QoS Implementation Techniques 299
QoS Implementation Techniques Overview 299
Traffic Marking Tools 299
Marking at Layer 2 300
Marking at Layer 3 300
QoS Mechanism Terminology 302
Check Your Understanding—QoS Implementation Techniques 303

Labs and Activities 304

Chapter 10 Network Management 305

Study Guide 306

Device Discovery with CDP and LLDP 306

Configure and Verify CDP 306
Configure and Verify LLDP 307
Draw and Label the Network Topology 308
Compare CDP and LLDP 309

NTP 310

Set the Clock 310
NTP Operation 310
Configure and Verify NTP 311

SNMP 311

SNMP Operation 311
SNMP Versions 312
Community Strings 312
MIB Object ID 312

Syslog 314
Introduction to Syslog 314
Syslog Operation 314
Syslog Message Format 314
Check Your Understanding—Syslog Operation 315

Router and Switch File Maintenance 315
Router File Systems 315
Use a Text File to Back Up a Configuration 317
Use a Text File to Restore a Configuration 318
Use TFTP to Back Up and Restore a Configuration 319
Use USB to Back Up and Restore a Configuration 319
Password Recovery Procedures 319
Labs and Packet Tracers 320

IOS Image Management 320
Video—Managing Cisco IOS Images 320
Back Up an IOS Image to a TFTP Server 320
The boot system Command 321

Labs and Activities 322

Command Reference 322

10.1.5 Packet Tracer—Use CDP to Map a Network (Instructor Version) 323
Addressing Table 323
Objectives 323
Background / Scenario 323
Instructions 324
Part 1: Use SSH to Remotely Access Network Devices 324
Part 2: Use CDP to Discover Neighboring Devices 324

10.2.6 Packet Tracer—Use LLDP to Map a Network (Instructor Version) 327
Addressing Table 327
Objectives 327
Background / Scenario 327
Instructions 328
Part 1: Use SSH to Remotely Access Network Devices 328
Part 2: Use LLDP to Discover Neighboring Devices 329

10.3.4 Packet Tracer—Configure and Verify NTP (Instructor Version) 332
Addressing Table 332
Objectives 332
Background / Scenario 332
Instructions 332

10.4.10 Lab—Research Network Monitoring Software (Instructor Version) 334
Objectives 334
Background / Scenario 334
Required Resources 334

Instructions 334
Part 1: Survey Your Understanding of Network Monitoring 334
Part 2: Research Network Monitoring Tools 335
Part 3: Select a Network Monitoring Tool 336
Reflection Question 336

10.6.10 Packet Tracer—Back Up Configuration Files (Instructor Version) 337

Objectives 337
Background / Scenario 337
Instructions 337
Part 1: Establish Connectivity to the TFTP Server 337
Part 2: Transfer the Configuration File from the TFTP Server 337
Part 3: Back Up Configuration and IOS to TFTP Server 338

10.6.11 Lab—Use Tera Term to Manage Router Configuration Files (Instructor Version) 340

Topology 340
Addressing Table 340
Objectives 340
Background / Scenario 340
Required Resources 341
Part 1: Configure Basic Device Settings 341
Part 2: Create a Backup Configuration File 343
Part 3: Use a Backup Configuration File to Restore a Router and Switch Configuration 343
Reflection Question 345
Router Interface Summary Table 345
Device Configs - Final 346
Router R1 346
Switch S1 348

10.6.12 Lab—Use TFTP, Flash, and USB to Manage Configuration Files (Instructor Version) 351

Topology 351
Addressing Table 351
Objectives 351
Background / Scenario 351
Required Resources 352
Instructions 352
Part 1: Build the Network and Configure Basic Device Settings 352
Part 2: Use TFTP to Back Up and Restore the Switch Running Configuration 354
Part 3: Use TFTP to Back Up and Restore the Router Running Configuration 358
Part 4: Back Up and Restore Configurations Using Router Flash Memory 358

Part 5: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration 361
Reflection Questions 363
Router Interface Summary Table 364
Device Configs 364
Router R1 364
Switch S1 366

10.6.13 Lab—Research Password Recovery Procedures (Instructor Version) 370

Objectives 370
Background / Scenario 370
Required Resources 370
Instructions 370
Part 1: Research the Configuration Register 370
Part 2: Document the Password Recovery Procedure for a Specific Cisco Router 372
Reflection Question 373

10.7.6 Packet Tracer—Use a TFTP Server to Upgrade a Cisco IOS Image (Instructor Version) 374

Addressing Table 374
Objectives 374
Scenario 374
Instructions 374
Part 1: Upgrade an IOS Image on a Cisco Device 374
Part 2: Back Up an IOS Image to a TFTP Server 376

10.8.1 Packet Tracer—Configure CDP, LLDP, and NTP (Instructor Version) 377

Addressing Table 377
Objectives 377
Background / Scenario 377
Instructions 378
Answer Scripts 378
Router HQ 378
Router Branch 379
Switch HQ-SW-1 379
Switch HQ-SW2 379
Switch BR-SW-2 380
Switch BR-SW-3 380

10.8.2 Lab—Configure CDP, LLDP, and NTP (Instructor Version) 381

Topology 381
Addressing Table 381
Objectives 381
Background / Scenario 381

Required Resources 382
Part 1: Build the Network and Configure Basic Device Settings 382
Part 2: Network Discovery with CDP 384
Part 3: Network Discovery with LLDP 386
Part 4: Configure NTP 388
Reflection Question 389
Router Interface Summary Table 389
Device Configs - Final 390
Router R1 390
Switch S1 392
Switch S2 395

Chapter 11 Network Design 399

Study Guide 400

Hierarchical Networks 400

Video—Three-Layer Network Design 400
Borderless Switched Networks 400
Hierarchy in the Borderless Switched Network 400
Access, Distribution, and Core Layer Functions 402
Check Your Understanding—Hierarchical Networks 403

Scalable Networks 403

Identify Scalability Terminology 404
Check Your Understanding—Scalable Networks 404

Switch Hardware 405

Switch Hardware Features 405
Check Your Understanding—Switch Hardware 406

Router Hardware 407

Router Categories 407
Check Your Understanding—Router Hardware 407

Labs and Activities 409

11.5.1 Packet Tracer—Compare Layer 2 and Layer 3 Devices (Instructor Version) 409

Objective 409
Background 409
Instructions 409

Chapter 12 Network Troubleshooting 413

Study Guide 414

Network Documentation 414

Documentation Overview 414
Network Topology Diagrams 414
Network Device Documentation 416
Establish a Network Baseline 418

Data Measurement 418
Check Your Understanding—Network Documentation 419

Troubleshooting Process 419

General Troubleshooting Procedures 420
Seven-Step Troubleshooting Process 421
Gather Information 421
Structured Troubleshooting Methods 422
Check Your Understanding—Troubleshooting Process 423

Troubleshooting Tools 425

Identify the Troubleshooting Tool 425
Syslog Server as a Troubleshooting Tool 426
Check Your Understanding—Troubleshooting Tools 426

Symptoms and Causes of Network Problems 427

Isolate the OSI Layer 427
Check Your Understanding—Symptoms and Causes of Network Problems 428

Troubleshooting IP Connectivity 429

Labs and Activities 431

12.5.13 Packet Tracer—Troubleshoot Enterprise Network (Instructor Version) 431

Objectives 431
Scenario 431
Addressing Table 431
Instructions 432
Part 1: Verify Switching Technologies 432
Part 2: Verify DHCP 434
Part 3: Verify Routing 435
Part 4: Verify WAN Technologies 436
Part 5: Verify Connectivity 438

12.6.1 Packet Tracer—Troubleshooting Challenge—Document the Network (Instructor Version) 439

Addressing Table 439
Objectives 440
Background / Scenario 440
Instructions 440
Part 1: Test Connectivity 440
Part 2: Discover PC Configuration Information 440
Part 3: Discover Information About the Default Gateway Devices 440
Part 4: Reconstruct the Network Topology 441
Part 5: Further Explore Device Configurations and Interconnections 441
Reflection 441
Network Topology Diagram 442

12.6.2 Packet Tracer—Troubleshooting Challenge—Use Documentation to Solve Issues (Instructor Version) 444

Addressing Table 444

Objectives 445

Background / Scenario 445

Instructions 445

Part 1: Assess Connectivity 445

Part 2: Access Network Devices 445

Part 3: Repair the Network 445

Part 4: Document the Issues 446

Chapter 13 Network Virtualization 449

Study Guide 450

Cloud Computing 450

Video—Cloud and Virtualization 450

Cloud Computing Terminology 450

Check Your Understanding—Cloud Computing 451

Virtualization and Virtual Network Infrastructure 451

Virtualization Terminology 452

Check Your Understanding—Virtualization and Virtual Network Infrastructure 452

Software-Defined Networking 453

Video—Software-Defined Networking 454

Control Plane and Data Plane 454

Check Your Understanding—Software-Defined Networking 454

Controllers 455

Video—Cisco ACI 455

Types of SDN Controllers 456

Check Your Understanding—Controllers 456

Labs and Activities 458

13.6.1 Lab—Install Linux in a Virtual Machine and Explore the GUI (Instructor Version) 458

Objectives 458

Background / Scenario 458

Required Resources 458

Instructions 458

Part 1: Prepare a Computer for Virtualization 458

Part 2: Install Ubuntu on the Virtual Machine 459

Part 3: Explore the GUI 461

Reflection Question 462

Chapter 14 Network Automation 463

Study Guide 464

Automation Overview 464

Video—Automation Everywhere 464

Check Your Understanding—Benefits of Automation 464

Data Formats 465

Video—Data Formats 465

Identify the Data Formats 465

Check Your Understanding—Data Formats 466

APIs 467

Video—APIs 467

An API Example 467

Types of Web Service APIs 467

Check Your Understanding—APIs 468

REST 469

Video—REST 469

RESTful Implementation 469

URI, URN, and URL 469

Anatomy of a RESTful Request 470

Check Your Understanding—REST 470

Configuration Management 471

Video—Configuration Management 471

Compare Ansible, Chef, Puppet, and SaltStack 471

Check Your Understanding—Configuration Management 472

IBN and Cisco DNA Center 473

Video—Intent-Based Networking 473

Intent-Based Networking Overview 473

Network Infrastructure as Fabric 474

Cisco Digital Network Architecture (DNA) 475

Cisco DNA Center 477

Videos—Cisco DNA Center 478

Check Your Understanding—IBN and Cisco DNA Center 478

Labs and Activities 479

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

This book supports instructors and students in Cisco Networking Academy, an IT skills and career-building program for learning institutions and individuals worldwide. Cisco Networking Academy provides a variety of curriculum choices, including the very popular CCNA curriculum. It includes three courses oriented around the topics of Cisco Certified Network Associate (CCNA) certifications.

Enterprise Networking, Security, and Automation Labs and Study Guide is a supplement to your classroom and laboratory experience with Cisco Networking Academy. To be successful on the exam and achieve your CCNA certification, you should do everything in your power to arm yourself with a variety of tools and training materials to support your learning efforts. This *Labs and Study Guide* provides just such a collection of tools. Used to its fullest extent, it will help you gain knowledge as well as practice skills associated with the content area of the Enterprise Networking, Security, and Automation v7 course. Specifically, this book will help you work on these main areas:

- Explain how single-area OSPF operates in both point-to-point and broadcast multiaccess networks.
- Implement single-area OSPFv2 in both point-to-point and broadcast multiaccess networks.
- Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.
- Explain how ACLs are used as part of a network security policy.
- Implement IPv4 ACLs to filter traffic and secure administrative access.
- Configure NAT services on the edge router to provide IPv4 address scalability.
- Explain how WAN access technologies can be used to satisfy business requirements.
- Explain how VPNs and IPsec secure site-to-site and remote access connectivity.
- Explain how networking devices implement QoS.
- Implement protocols to manage the network.
- Explain the characteristics of scalable network architectures.
- Troubleshoot enterprise networks.
- Explain the purpose and characteristics of network virtualization.
- Explain how network automation is enabled through RESTful APIs and configuration management tools.

Labs and Study Guide similar to this one are also available for the other two courses: *Introduction to Networks Labs and Study Guide* and *Switching, Routing, and Wireless Essentials Labs and Study Guide*.

Who Should Read This Book

This book's main audience is anyone taking the Enterprise Networking, Security, and Automation course of the Cisco Networking Academy curriculum. Many Academies use this *Labs and Study Guide* as a required tool in the course; other Academies recommend the *Labs and Study Guide* as an additional resource to prepare for class exams and the CCNA certification.

The secondary audiences for this book include people taking CCNA-related classes from professional training organizations, those in college- and university-level networking courses, and anyone wanting to gain a detailed understanding of routing. However, the reader should know that the content of this book tightly aligns with the Cisco Networking Academy course. It may not be possible to complete some of the "Study Guide" sections and Labs without access to the online course. Fortunately, you can purchase the *Enterprise Networking, Security, and Automation v7.0 Companion Guide* (ISBN: 9780136634324).

Goals and Methods

The most important goal of this book is to help you pass the 200-301 Cisco Certified Network Associate exam, which is associated with the Cisco Certified Network Associate (CCNA) certification. Passing the CCNA exam means that you have the knowledge and skills required to manage a small, enterprise network. You can view the detailed exam topics at http://learningnetwork.cisco.com. They are divided into six broad categories:

- Network Fundamentals
- Network Access
- IP Connectivity
- IP Services
- Security Fundamentals
- Automation and Programmability

The Enterprise Networking, Security, and Automation v7 course covers introductory material in the last four bullets. The previous two courses, Introduction to Networks v7 and Switching, Routing, and Wireless Essentials v7, cover the material in the first two bullets.

Each chapter of this book is divided into a "Study Guide" section followed by a "Labs and Activities" section. The "Study Guide" section offers exercises that help you learn the concepts, configurations, and troubleshooting skills crucial to your success as a CCNA exam candidate. Each chapter is slightly different and includes some or all of the following types of exercises:

- Vocabulary matching exercises
- Concept questions exercises
- Skill-building activities and scenarios
- Configuration scenarios
- Packet Tracer exercises
- Troubleshooting scenarios

The "Labs and Activities" sections include all the online course labs and Packet Tracer activity instructions. If applicable, this section begins with a Command Reference that you will complete to highlight all the commands introduced in the chapter.

Packet Tracer and Companion Website

This book includes the instructions for all the Packet Tracer activities in the online course. You need to be enrolled in the Enterprise Networking, Security, and Automation Companion Guide v7 course to access these Packet Tracer files.

Four Packet Tracer activities have been created exclusively for this book. You can access these unique Packet Tracer files at this book's companion website.

To get your copy of Packet Tracer software and the four unique files for this book, please go to the companion website for instructions. 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: 9780136634690.

Step 3. Answer the challenge question as proof of purchase.

Step 4. Click on 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.

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Switching, Routing, and Wireless Essentials v7 course and is divided into 14 chapters:

- **Chapter 1, "Single-Area OSPFv2 Concepts":** This chapter reviews single-area OSPF. It describes basic OSPF features and characteristics, packet types, and single-area operation.
- **Chapter 2, "Single-Area OSPFv2 Configuration":** This chapter reviews how to implement single-area OSPFv2 networks. It includes router ID configuration, point-to-point configuration, DR/BDR election, single-area modification, default route propagation, and verification of single-area OSPFv2 configuration.
- **Chapter 3, "Network Security Concepts":** This chapter reviews how vulnerabilities, threats, and exploits can be mitigated to enhance network security. It includes descriptions of the current state of cybersecurity, tools used by threat actors, malware types, common network attacks, IP vulnerabilities, TCP and UDP vulnerabilities, network best practices, and cryptography.
- **Chapter 4, "ACL Concepts":** This chapter reviews how ACLs are used to filter traffic, how wildcard masks are used, the creation of ACLs, and the difference between standard and extended IPv4 ACLs.
- **Chapter 5, "ACLs for IPv4 Configuration":** This chapter reviews how to implement ACLs. It includes standard IPv4 ACL configuration, ACL modifications using sequence numbers, applying an ACL to vty lines, and extended IPv4 ACL configuration.
- **Chapter 6, "NAT for IPv4":** This chapter reviews how to enable NAT services on a router to provide IPv4 address scalability. It includes descriptions of the purpose and function of NAT, the different types of NAT, and the advantages and disadvantages of NAT. Configuration topics include static NAT, dynamic NAT, and PAT. NAT64 is also briefly discussed.
- **Chapter 7, "WAN Concepts":** This chapter reviews how WAN access technologies can be used to satisfy business requirements. It includes descriptions of the purpose of a WAN, how WANs operate, traditional WAN connectivity options, modern WAN connectivity options, and internet-based connectivity options.
- **Chapter 8, "VPN and IPsec Concepts":** This chapter reviews how VPNs and IPsec are used to secure communications. It includes descriptions of different types of VPNs and an explanation of how the IPsec framework is used to secure network traffic.

- **Chapter 9, "QoS Concepts":** This chapter reviews how network devices use QoS to prioritize network traffic. It includes descriptions of network transmission characteristics, queuing algorithms, different queueing models, and QoS implementation techniques.
- **Chapter 10, "Network Management":** This chapter reviews how to use a variety of protocols and techniques to manage the network, including CDP, LLDP, NTP, SNMP, and syslog. In addition, this chapter discusses the management of configuration files and IOS images.
- **Chapter 11, "Network Design":** This chapter reviews the characteristics of scalable networks. It includes descriptions of network convergence, considerations for designing scalable networks, and switch and router hardware.
- **Chapter 12, "Network Troubleshooting":** This chapter reviews how to troubleshoot networks. It includes explanations of network documentation, troubleshooting methods, and troubleshooting tools. This chapter also demonstrates how to troubleshoot symptoms and causes of network problems using a layered approach.
- **Chapter 13, "Network Virtualization":** This chapter reviews the purpose and characteristics of network virtualization. It includes descriptions of cloud computing, the importance of virtualization, network device virtualization, software-defined network, and controllers used in network programming.
- **Chapter 14, "Network Automation":** This chapter reviews network automation. It includes descriptions of automation, data formats, APIs, REST, configuration management tools, and Cisco DNA Center.

CHAPTER 1

Single-Area OSPFv2 Concepts

The "Study Guide" portion of this chapter uses a variety of exercises to test your knowledge of how single-area Open Shortest Path First (OSPF) operates in both point-to-point and broadcast multiaccess networks. There are no labs or Packet Tracer activities for this chapter.

As you work through this chapter, use Chapter 1 in *Enterprise Networking, Security, and Automation v7 Companion Guide* or use the corresponding Module 1 in the Enterprise Networking, Security, and Automation online curriculum for assistance.

Study Guide

OSPF Features and Characteristics

In this section, you review basic OSPF features and characteristics.

Components of OSPF

OSPF is a link-state routing protocol that was developed as an alternative for the distance vector protocol Routing Information Protocol (RIP). OSPF uses the concept of areas. A network administrator can divide the routing domain into distinct areas that help control routing update traffic. A link is an interface on a router. Information about the state of a link is known as link-state information; this information includes the network prefix, prefix length, and cost.

The components of OSPF include

- **Router protocol messages:** OSPF routers exchange routing information using five types of packets. List them.
  - Hello packet
  - Database description packet
  - Link-state request packet
  - Link-state update packet
  - Link-state acknowledgment packet
- **Data structures:** OSPF messages are used to create and maintain three OSPF databases. List and briefly describe each of them in a few words.
  - **Adjacency database:** This creates the neighbor table.
  - **Link-state database (LSDB):** This creates the topology table.
  - **Forwarding database:** This creates the routing table.
- **Algorithm:** OSPF route calculations are based on Dijkstra's shortest-path first (SPF) algorithm, which accumulates the cost to reach a destination. This algorithm then builds a tree that is used to calculate the best routes to install in the routing table.

Link-State Operation

OSPF routers use the link-state routing process to reach a state of convergence where the LSDBs of all routers in the area have the same topology table. List and briefly describe the five steps in the link-state routing process.

Step 1. **Establish neighbor adjacencies:** Routers send Hello packets out all OSPF-enabled interfaces to attempt to establish a neighbor adjacency with any other OSPF-enabled routers.

Step 2. **Exchange link-state advertisements:** Routers exchange link-state advertisements (LSAs). LSAs contain the state and cost of each directly connected link.

Step 3. **Build the link state:** Routers build the topology table (LSDB) based on the received LSAs.

Step 4. **Execute the SPF algorithm:** Routers execute the SPF algorithm, which creates the SPF tree.

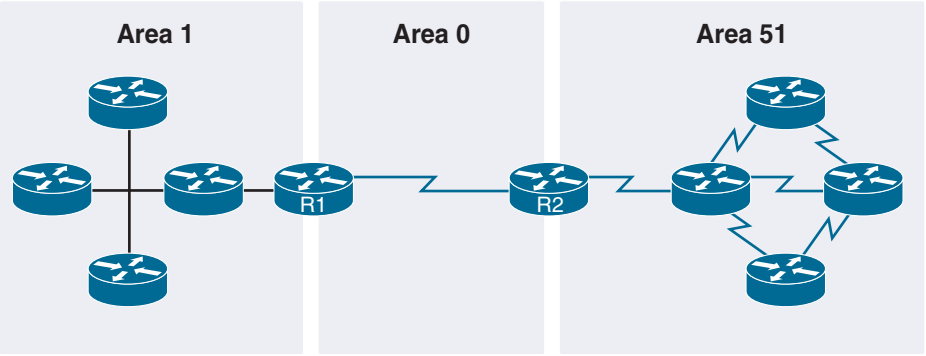
Step 5. **Choose the best route:** The best paths to each network are inserted into the routing table unless there is a route source to the same network with a lower administrative distance.

Single-Area and Multiarea OSPF

OSPF can be implemented in one of two ways:

- **Single-area OSPF:** All routers are in one area. Best practice is to use area 0.
- **Multiarea OSPF:** OSPF is implemented using multiple areas, in a hierarchical fashion. All areas must connect to the backbone area (area 0), as shown in Figure 1-1. Routers interconnecting the areas are referred to as area border routers (ABRs).

Figure 1-1 A Multiarea OSPF Topology



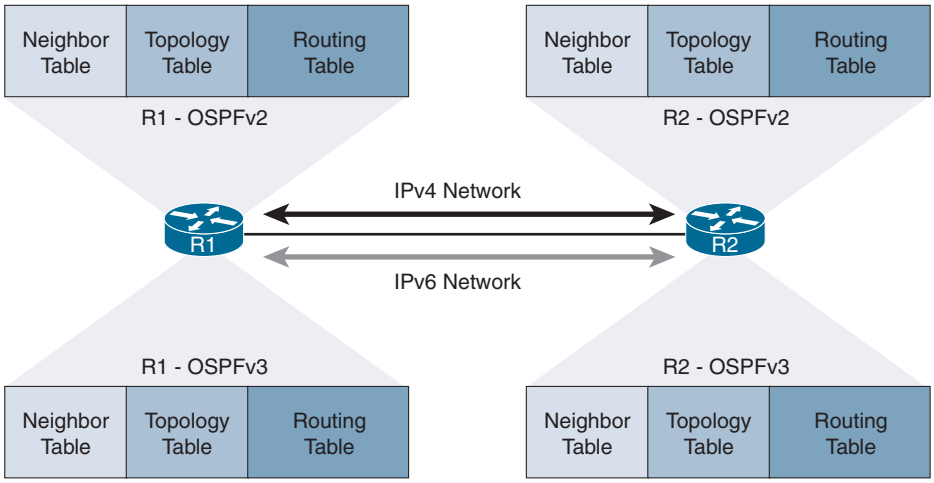
List and briefly describe three advantages of using multiarea OSPF.

- **Smaller routing tables:** With multiarea OSPF, network addresses can be summarized between areas.
- **Reduced link-state update overhead:** Designing multiarea OSPF with smaller areas minimizes processing and memory requirements.
- **Reduced frequency of SPF calculations:** Multiarea OSPF localize the impact of a topology change within an area.

OSPFv3

OSPFv3 is the version of OSPF used for exchanging IPv6 prefixes. OSPFv3 has the same functionality as OSPFv2 but uses IPv6 as the network layer transport, communicating with OSPFv3 peers and advertising IPv6 routes. OSPFv3 also uses the SPF algorithm as the computation engine to determine the best paths throughout the routing domain. OSPFv2 and OSPFv3 each have separate adjacency tables, OSPF topology tables, and IP routing tables, as shown in Figure 1-2.

Figure 1-2 OSPFv2 and OSPFv3 Data Structures



Check Your Understanding—OSPF Features and Characteristics

Check your understanding of OSPF features and characteristics by choosing the BEST answer to each of the following questions.

1. Which of the following OSPF components is associated with the neighbor table?

   a. Dijkstra's algorithm
   b. Link-state database
   c. Routing protocol messages
   d. Adjacency database
   e. Forwarding database

2. Which of the following OSPF components is responsible for computing the cost of each route?

   a. Dijkstra's algorithm
   b. Link-state database
   c. Routing protocol messages
   d. Adjacency database
   e. Forwarding database

3. Which of the following OSPF components is associated with the topology table?

   a. Dijkstra's algorithm
   b. Link-state database
   c. Routing protocol messages
   d. Adjacency database
   e. Forwarding database

4. Which of the following OSPF components is associated with the routing table?
   a. Dijkstra's algorithm
   b. Link-state database
   c. Routing protocol messages
   d. Adjacency database
   e. Forwarding database

Answers: 1 D; 2 A; 3 B; 4 E

OSPF Packets

In this section, you review how OSPF packet types are used in single-area OSPF.

Types of OSPF Packets

The following list describes the five different types of OSPF packets. Each packet serves a specific purpose in the OSPF routing process. Fill in the name for each packet type.

- **Hello**: Used to establish and maintain adjacency with other OSPF routers
- **Database Description (DBD)**: Contains an abbreviated list of the sending router's link-state database and is used by receiving routers to check against the local link-state database
- **Link-State Request (LSR)**: A request for more information about any entry in the DBD
- **Link-State Update (LSU)**: Used to reply to LSRs as well as to announce new information
- **Link-State Acknowledgment (LSAck)**: Confirms receipt of an LSU

Link-State Updates

Receiving an OSPF Hello packet on an interface confirms for a router that there is another OSPF router on the link. OSPF then begins the process of establishing adjacency with the neighbor.

Routers initially exchange Type 2 DBD packets. This type of packet is an abbreviated list of the sending router's LSDB and is used by receiving routers to check against the local LSDB.

The receiving routers use a Type 3 LSR packet to request more information about an entry in the DBD.

The Type 4 LSU packet is used to reply to an LSR packet.

Then, a Type 5 LSAck packet is sent to acknowledge receipt of the LSU.

In Table 1-1, indicate which OSPF packet type matches each LSA purpose.

Table 1-1 Identify OSPF Packet Types

LSA Purpose	OSPF Packet Type				
	Hello	DBD	LSR	LSU	LSAck
Discovers neighbors and builds adjacencies between them.	X				
Data field is empty.					X
Asks for specific link-state records from router to router.			X		
Sends specifically requested link-state records.				X	
Contains a list of the sending router's LSDB.		X			
Can contain seven different types of LSAs.			X		
Checks for database synchronization between routers.		X			
Confirms receipt of a link-state update packet.					X
Maintains adjacency with other OSPF routers.	X				

Hello Packet

Every OSPF message includes the header, as shown in Figure 1-3. Also shown in the figure are the fields of the OSPF Hello packet. Fill in the missing field names.

Figure 1-3 OSPF Message Format

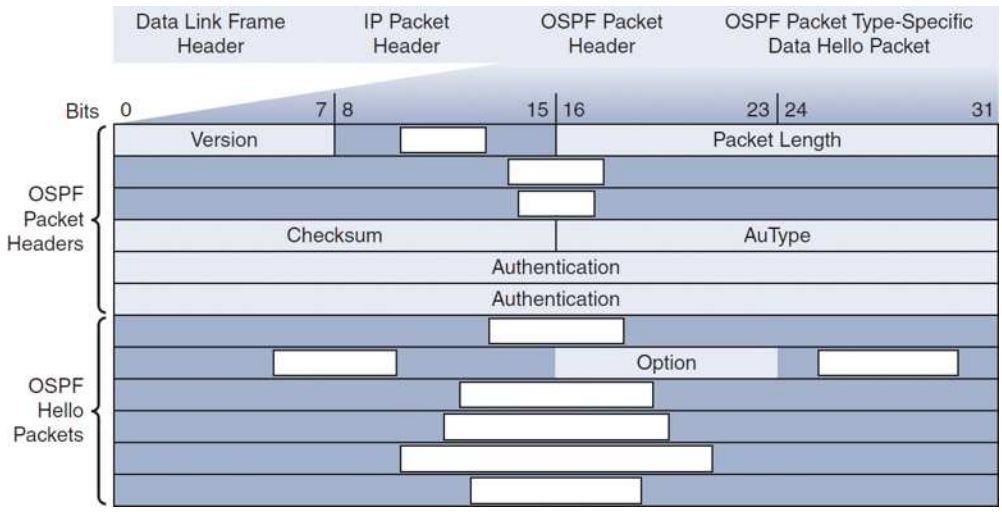
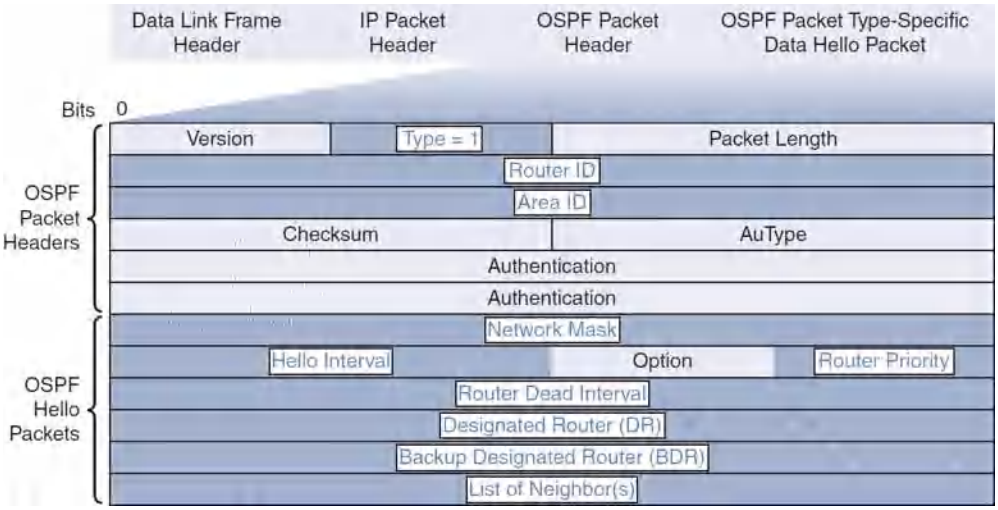


Figure 1-3a OSPF Message Format (answer)



Check Your Understanding—OSPF Packets

Check your understanding of OSPF packets by choosing the BEST answer to each of the following questions.

1. Which of the following OSPF packets contains an abbreviated list of the LSDB of the sending router?

   a. Type 1: Hello packet
   b. Type 2: DBD packet
   c. Type 3: LSR packet
   d. Type 4: LSU packet
   e. Type 5: LSAck packet

2. Which of the following OSPF packets do routers use to announce new information?

   a. Type 1: Hello packet
   b. Type 2: DBD packet
   c. Type 3: LSR packet
   d. Type 4: LSU packet
   e. Type 5: LSAck packet

3. Which of the following OSPF packets do routers use to request more information?

   a. Type 1: Hello packet
   b. Type 2: DBD packet
   c. Type 3: LSR packet
   d. Type 4: LSU packet
   e. Type 5: LSAck packet

4. Which of the following OSPF packets is responsible for establishing and maintaining adjacency with other OSPF routers?

   a. Type 1: Hello packet
   b. Type 2: DBD packet
   c. Type 3: LSR packet
   d. Type 4: LSU packet
   e. Type 5: LSAck packet

5. Which of the following OSPF packets is used to confirm receipt of an LSA?

   a. Type 1: Hello packet
   b. Type 2: DBD packet
   c. Type 3: LSR packet
   d. Type 4: LSU packet
   e. Type 5: LSAck packet

6. Which of the following is used with a Hello packet to uniquely identify the originating router?

   a. Hello Interval
   b. Router ID
   c. Designated Router ID
   d. Network Mask
   e. Dead Interval

Answers: 1 B; 2 D; 3 C; 4 A; 5 E; 6 B

OSPF Operation

In this section, you review how single-area OSPF operates.

OSPF Operational States

When an OSPF router is initially connected to a network, it attempts to

- Create adjacencies with neighbors
- Exchange routing information
- Calculate the best routes
- Reach convergence

In Figure 1-4, record the five states that occur between the *Down state* and the *Full state*.

Figure 1-4 Transitioning Through the OSPF States

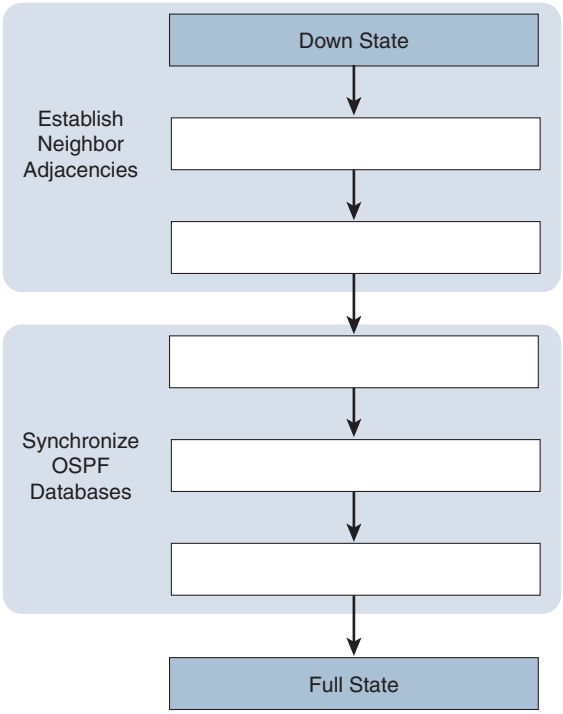
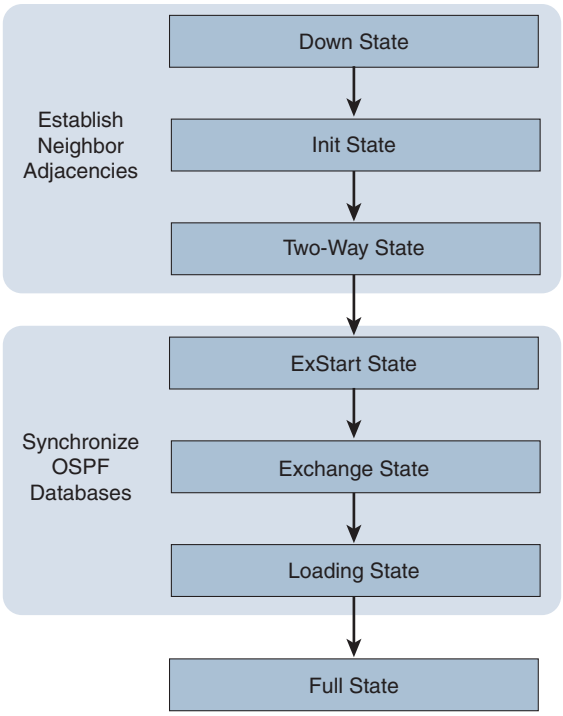


Figure 1-4a Transitioning Through the OSPF States (answer)



In Table 1-2, indicate which OSPF state matches each state description.

Table 1-2 Identify the OSPF States

State Description	OSPF States						
	Down	Init	Two-Way	Ex-Start	Exchange	Loading	Full
Routes are processed using the SPF algorithm.						X	
A neighbor responds to a Hello.		X					
Hello packets are received from neighbors and contain the sending router ID.		X					
On Ethernet links, elect a designated router (DR) and a backup designated router (BDR).			X				
No Hello packets received.	X						
Router requests more information about a specific DBD entry.						X	
Routers exchange DBD packets.					X		
Routers have converged.							X
The LSDB and routing tables are complete.							X
A new OSPF router on the link sends the first Hello.		X					
Exchange of DBD packets initiated.					X		
Negotiation of the master/slave relationship and DBD packet sequence number.				X			

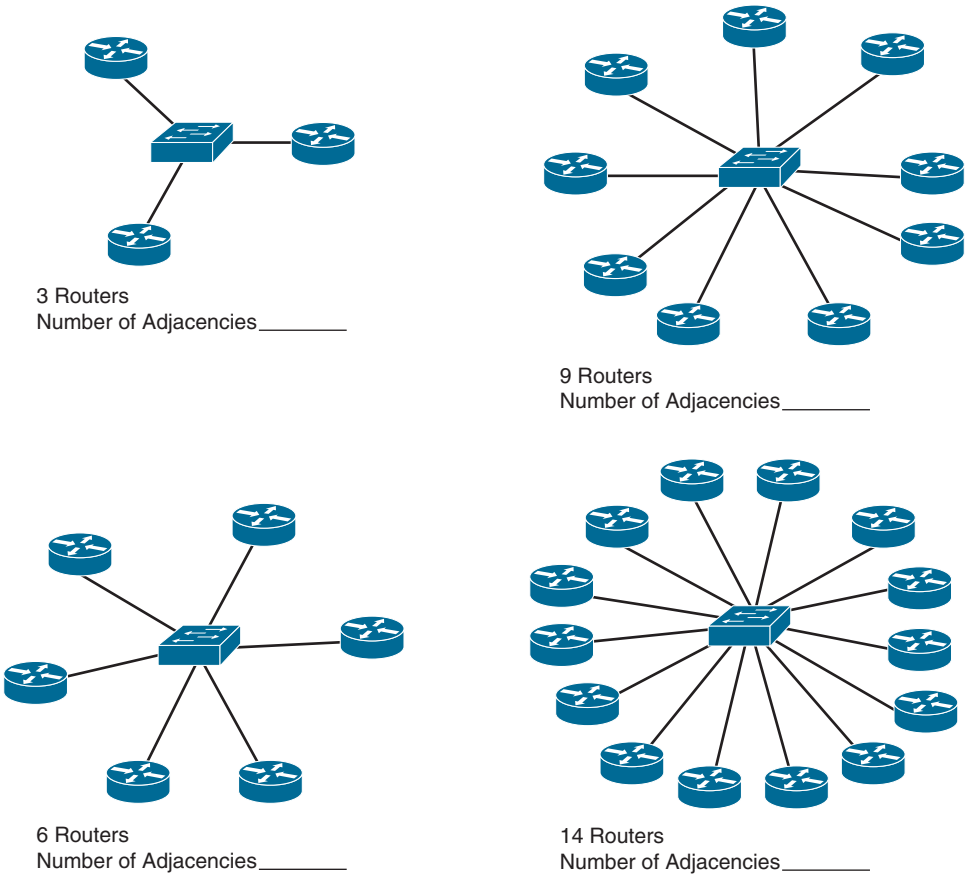
The Need for a DR

Describe the two challenges regarding OSPF LSA flooding in multiaccess networks.

- **Creation of multiple adjacencies:** Creating adjacencies with every router is unnecessary and undesirable. It would lead to an excessive number of LSAs being exchanged between routers on the same network.
- **Extensive flooding of LSAs:** Link-state routers flood their LSAs any time OSPF is initialized or when there is a change in the topology. This flooding can become excessive.

For each multiaccess topology in Figure 1-5, indicate how many adjacencies would be formed if the DB/BDR process were not part of OSPF operations.

Figure 1-5 Multiaccess Topologies



Answers: 3 routers: 3(3 – 1) / 2 = 3 adjacencies; 6 routers: 6(6 – 1)/2 = 15 adjacencies; 9 routers = 9(9 – 1) / 2 = 36 adjacencies; 14 routers = 14(14 – 1) / 2 = 91 adjacencies

LSA Flooding with a DR

Briefly describe how the designated router (DR) reduces the impact of LSA flooding.

On multiaccess networks, OSPF elects a DR to be the collection and distribution point for LSAs sent and received. A BDR is also elected in case the DR fails. All other routers become DROTHERs. A DROTHER is a router that is neither the DR nor the BDR.

Check Your Understanding—OSPF Operation

Check your understanding of OSPF operation by choosing the BEST answer to each of the following questions.

1. During this OSPF state on multiaccess networks, the routers elect a designated router (DR) and a backup designated router (BDR).

   a. Down state
   b. Init state
   c. Two-Way state
   d. ExStart state
   e. Exchange state
   f. Loading state
   g. Full state

2. During this OSPF state, routers send each other DBD packets.

   a. Down state
   b. Init state
   c. Two-Way state
   d. ExStart state
   e. Exchange state
   f. Loading state
   g. Full state

3. An OSPF router enters this state when it has received from a neighbor a Hello packet that contains the sending router's router ID.

   a. Down state
   b. Init state
   c. Two-Way state
   d. ExStart state
   e. Exchange state
   f. Loading state
   g. Full state

4. During this OSPF state on point-to-point networks, the routers decide which router initiates the exchange of DBD packets.
   a. Down state
   b. Init state
   c. Two-Way state
   d. ExStart state
   e. Exchange state
   f. Loading state
   g. Full state
5. During this OSPF state, routers have converged link-state databases.
   a. Down state
   b. Init state
   c. Two-Way state
   d. ExStart state
   e. Exchange state
   f. Loading state
   g. Full state
6. During this OSPF state, no Hello packets are received.
   a. Down state
   b. Init state
   c. Two-Way state
   d. ExStart state
   e. Exchange state
   f. Loading state
   g. Full state
7. During this OSPF state, the link-state databases are fully synchronized.
   a. Down state
   b. Init state
   c. Two-Way state
   d. ExStart state
   e. Exchange state
   f. Loading state
   g. Full state

Answers: 1 C; 2 E; 3 B; 4 D; 5 G; 6 A; 7 F