



CCNAv7: Enterprise Networking, Security, and Automation

Companion Guide



Enterprise Networking, Security, and Automation Companion Guide (CCNAv7)

Cisco Press

Enterprise Networking, Security, and Automation Companion Guide (CCNAv7)

Cisco Networking Academy

Copyright© 2020 Cisco Systems, Inc.

Published by:
Cisco Press

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

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020935515

ISBN-13: 978-0-13-663432-4

ISBN-10: 0-13-663432-X

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Enterprise Networking, Security, and Automation (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.

Editor-in-Chief
Mark Taub

Alliances Manager,
Cisco Press
Arezou Gol

Director, ITP Product
Management
Brett Bartow

Senior Editor
James Manly

Managing Editor
Sandra Schroeder

Development Editor
Ellie Bru

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Technical Editor
Bob Vachon

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Ken Johnson

Proofreader
Betty Pessagno

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



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.

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 Contributing Authors

Bob Vachon is a professor at Cambrian College (Sudbury, Ontario) and Algonquin College (Ottawa, Ontario). He has more than 30 years of computer, networking, and information technology teaching experience and has collaborated on many Cisco Networking Academy courses, including CCNA, CCNA Security, CCNP, Cybersecurity, and more as team lead, lead author, and subject matter expert. Bob enjoys playing guitar by a campfire with friends and family.

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.

Contents at a Glance

	Introduction	xxxi
Chapter 1	Single-Area OSPFv2 Concepts	1
Chapter 2	Single-Area OSPFv2 Configuration	33
Chapter 3	Network Security Concepts	93
Chapter 4	ACL Concepts	163
Chapter 5	ACLs for IPv4 Configuration	187
Chapter 6	NAT for IPv4	225
Chapter 7	WAN Concepts	269
Chapter 8	VPN and IPsec Concepts	319
Chapter 9	QoS Concepts	351
Chapter 10	Network Management	389
Chapter 11	Network Design	453
Chapter 12	Network Troubleshooting	501
Chapter 13	Network Virtualization	581
Chapter 14	Network Automation	617
Appendix A	Answers to the “Check Your Understanding” Questions	657
	Glossary	677
	Index	715

Contents

Introduction xxxi

Chapter 1 Single-Area OSPFv2 Concepts 1

Objectives 1

Key Terms 1

Introduction (1.0) 3

OSPF Features and Characteristics (1.1) 3

Introduction to OSPF (1.1.1) 3

Components of OSPF (1.1.2) 4

Routing Protocol Messages 4

Data Structures 4

Algorithm 5

Link-State Operation (1.1.3) 6

1. Establish Neighbor Adjacencies 6

2. Exchange Link-State Advertisements 6

3. Build the Link-State Database 7

4. Execute the SPF Algorithm 8

5. Choose the Best Route 8

Single-Area and Multiarea OSPF (1.1.4) 9

Multiarea OSPF (1.1.5) 10

OSPFv3 (1.1.6) 12

OSPF Packets (1.2) 13

Types of OSPF Packets (1.2.2) 13

Link-State Updates (1.2.3) 14

Hello Packet (1.2.4) 15

OSPF Operation (1.3) 17

OSPF Operational States (1.3.2) 17

Establish Neighbor Adjacencies (1.3.3) 18

1. Down State to Init State 18

2. The Init State 19

3. Two-Way State 19

4. Elect the DR and BDR 20

Synchronizing OSPF Databases (1.3.4) 20

1. Decide First Router 21

2. Exchange DBDs 21

3. Send an LSR 22

The Need for a DR (1.3.5) 23

	LSA Flooding with a DR (1.3.6)	24
	<i>Flooding LSAs</i>	24
	<i>LSAs and DR</i>	25
	Summary (1.4)	27
	OSPF Features and Characteristics	27
	OSPF Packets	28
	OSPF Operation	28
	Practice	29
	Check Your Understanding	29
Chapter 2	Single-Area OSPFv2 Configuration	33
	Objectives	33
	Key Terms	33
	Introduction (2.0)	34
	OSPF Router ID (2.1)	34
	OSPF Reference Topology (2.1.1)	34
	Router Configuration Mode for OSPF (2.1.2)	35
	Router IDs (2.1.3)	36
	Router ID Order of Precedence (2.1.4)	36
	Configure a Loopback Interface as the Router ID (2.1.5)	37
	Explicitly Configure a Router ID (2.1.6)	38
	Modify a Router ID (2.1.7)	39
	Point-to-Point OSPF Networks (2.2)	40
	The network Command Syntax (2.2.1)	40
	The Wildcard Mask (2.2.2)	41
	Configure OSPF Using the network Command (2.2.4)	41
	Configure OSPF Using the ip ospf Command (2.2.6)	43
	Passive Interface (2.2.8)	44
	Configure Passive Interfaces (2.2.9)	45
	OSPF Point-to-Point Networks (2.2.11)	46
	Loopbacks and Point-to-Point Networks (2.2.12)	48
	Multiaccess OSPF Networks (2.3)	49
	OSPF Network Types (2.3.1)	49
	OSPF Designated Router (2.3.2)	49
	OSPF Multiaccess Reference Topology (2.3.3)	51
	Verify OSPF Router Roles (2.3.4)	52

<i>R1 DROTHER</i>	52
<i>R2 BDR</i>	53
<i>R3 DR</i>	53
Verify DR/BDR Adjacencies (2.3.5)	54
<i>R1 Adjacencies</i>	55
<i>R2 Adjacencies</i>	55
<i>R3 Adjacencies</i>	56
Default DR/BDR Election Process (2.3.6)	56
DR Failure and Recovery (2.3.7)	58
<i>R3 Fails</i>	58
<i>R3 Rejoins Network</i>	59
<i>R4 Joins Network</i>	59
<i>R2 Fails</i>	59
The ip ospf priority Command (2.3.8)	61
Configure OSPF Priority (2.3.9)	61
Modify Single-Area OSPFv2 (2.4)	63
Cisco OSPF Cost Metric (2.4.1)	63
Adjust the Reference Bandwidth (2.4.2)	64
OSPF Accumulates Costs (2.4.3)	66
Manually Set OSPF Cost Value (2.4.4)	67
Test Failover to Backup Route (2.4.5)	69
Hello Packet Intervals (2.4.7)	69
Verify Hello and Dead Intervals (2.4.8)	70
Modify OSPFv2 Intervals (2.4.9)	71
Default Route Propagation (2.5)	73
Propagate a Default Static Route in OSPFv2 (2.5.1)	74
Verify the Propagated Default Route (2.5.2)	75
Verify Single-Area OSPFv2 (2.6)	77
Verify OSPF Neighbors (2.6.1)	77
Verify OSPF Protocol Settings (2.6.2)	79
Verify OSPF Process Information (2.6.3)	80
Verify OSPF Interface Settings (2.6.4)	81
Summary (2.7)	83
OSPF Router ID	83
Point-to-Point OSPF Networks	83
OSPF Network Types	84
Modify Single-Area OSPFv2	85

	Default Route Propagation	86
	Verify Single-Area OSPFv2	86
	Practice	87
	Check Your Understanding	88
Chapter 3	Network Security Concepts	93
	Objectives	93
	Key Terms	93
	Introduction	95
	Ethical Hacking Statement (3.0.3)	95
	Current State of Cybersecurity (3.1)	95
	Current State of Affairs (3.1.1)	95
	Vectors of Network Attacks (3.1.2)	96
	Data Loss (3.1.3)	97
	Threat Actors (3.2)	98
	The Hacker (3.2.1)	98
	Evolution of Hackers (3.2.2)	99
	Cyber Criminals (3.2.3)	100
	Hacktivists (3.2.4)	100
	State-Sponsored Hackers (3.2.5)	100
	Threat Actor Tools (3.3)	101
	Introduction to Attack Tools (3.3.2)	101
	Evolution of Security Tools (3.3.3)	102
	Attack Types (3.3.4)	104
	Malware (3.4)	106
	Overview of Malware (3.4.1)	106
	Viruses and Trojan Horses (3.4.2)	106
	Other Types of Malware (3.4.3)	108
	Common Network Attacks (3.5)	109
	Overview of Network Attacks (3.5.1)	109
	Reconnaissance Attacks (3.5.3)	109
	Access Attacks (3.5.5)	110
	<i>Trust Exploitation Example</i>	111
	<i>Port Redirection Example</i>	112
	<i>Man-in-the-Middle Attack Example</i>	112
	<i>Buffer Overflow Attack</i>	112
	Social Engineering Attacks (3.5.6)	114

DoS and DDoS Attacks (3.5.9) 115

DoS Attack 116

DDoS Attack 116

IP Vulnerabilities and Threats (3.6) 117

IPv4 and IPv6 (3.6.2) 118

ICMP Attacks (3.6.3) 118

Amplification and Reflection Attacks (3.6.5) 119

Address Spoofing Attacks (3.6.6) 120

TCP and UDP Vulnerabilities (3.7) 122

TCP Segment Header (3.7.1) 122

TCP Services (3.7.2) 123

TCP Attacks (3.7.3) 124

TCP SYN Flood Attack 124

TCP Reset Attack 125

TCP Session Hijacking 126

UDP Segment Header and Operation (3.7.4) 126

UDP Attacks (3.7.5) 127

UDP Flood Attacks 127

IP Services 127

ARP Vulnerabilities (3.8.1) 127

ARP Cache Poisoning (3.8.2) 128

ARP Request 128

ARP Reply 129

Spoofed Gratuitous ARP Replies 130

DNS Attacks (3.8.4) 131

DNS Open Resolver Attacks 131

DNS Stealth Attacks 132

DNS Domain Shadowing Attacks 132

DNS Tunneling (3.8.5) 132

DHCP (3.8.6) 133

DHCP Attacks (3.8.7) 134

1. Client Broadcasts DHCP Discovery Messages 134

2. DHCP Servers Respond with Offers 134

3. Client Accepts Rogue DHCP Request 136

4. Rogue DHCP Acknowledges the Request 136

Network Security Best Practices (3.9) 137

Confidentiality, Integrity, and Availability (3.9.1) 137

The Defense-in-Depth Approach (3.9.2) 138

Firewalls (3.9.3) 139

IPS (3.9.4)	140
Content Security Appliances (3.9.5)	141
<i>Cisco Email Security Appliance (ESA)</i>	142
<i>Cisco Web Security Appliance (WSA)</i>	142

Cryptography (3.10) 143

Securing Communications (3.10.2)	143
Data Integrity (3.10.3)	144
Hash Functions (3.10.4)	145
<i>MD5 with 128-Bit Digest</i>	145
<i>SHA Hashing Algorithm</i>	146
SHA-2	146
SHA-3	146
Origin Authentication (3.10.5)	147
<i>HMAC Hashing Algorithm</i>	147
<i>Creating the HMAC Value</i>	148
<i>Verifying the HMAC Value</i>	149
<i>Cisco Router HMAC Example</i>	149
Data Confidentiality (3.10.6)	150
Symmetric Encryption (3.10.7)	151
Asymmetric Encryption (3.10.8)	152
Diffie-Hellman (3.10.9)	155

Summary (3.11) 157

Current State of Cybersecurity	157
Threat Actors	157
Threat Actor Tools	157
Malware	157
Common Network Attacks	158
IP Vulnerabilities and Threats	158
TCP and UDP Vulnerabilities	158
IP Services	158
Network Security Best Practices	159
Cryptography	159

Practice 159**Check Your Understanding 160**

Chapter 4	ACL Concepts 163
	Objectives 163
	Key Terms 163

Introduction (4.0) 164

Purpose of ACLs (4.1) 164

What Is an ACL? (4.1.1) 164

Packet Filtering (4.1.2) 165

ACL Operation (4.1.3) 166

Wildcard Masks in ACLs (4.2) 168

Wildcard Mask Overview (4.2.1) 168

Wildcard Mask Types (4.2.2) 169

Wildcard to Match a Host 169

Wildcard Mask to Match an IPv4 Subnet 169

Wildcard Mask to Match an IPv4 Address Range 170

Wildcard Mask Calculation (4.2.3) 170

Example 1 171

Example 2 171

Example 3 171

Example 4 172

Wildcard Mask Keywords (4.2.4) 172

Guidelines for ACL Creation (4.3) 173

Limited Number of ACLs per Interface (4.3.1) 173

ACL Best Practices (4.3.2) 174

Types of IPv4 ACLs (4.4) 175

Standard and Extended ACLs (4.4.1) 175

Numbered and Named ACLs (4.4.2) 176

Numbered ACLs 176

Named ACLs 177

Where to Place ACLs (4.4.3) 177

Standard ACL Placement Example (4.4.4) 179

Extended ACL Placement Example (4.4.5) 180

Summary (4.5) 182

Purpose of ACLs 182

Wildcard Masks 182

Guidelines for ACL Creation 183

Types of IPv4 ACLs 183

Practice 184

Check Your Understanding Questions 184

Chapter 5	ACLs for IPv4 Configuration	187
	Objectives	187
	Key Term	187
	Introduction (5.0)	188
	Configure Standard IPv4 ACLs (5.1)	188
	Create an ACL (5.1.1)	188
	Numbered Standard IPv4 ACL Syntax (5.1.2)	188
	Named Standard IPv4 ACL Syntax (5.1.3)	189
	Apply a Standard IPv4 ACL (5.1.4)	190
	Numbered Standard IPv4 ACL Example (5.1.5)	191
	Named Standard IPv4 ACL Example (5.1.6)	193
	Modify IPv4 ACLs (5.2)	195
	Two Methods to Modify an ACL (5.2.1)	196
	Text Editor Method (5.2.2)	196
	Sequence Numbers Method (5.2.3)	197
	Modify a Named ACL Example (5.2.4)	198
	ACL Statistics (5.2.5)	199
	Secure VTY Ports with a Standard IPv4 ACL (5.3)	200
	The access-class Command (5.3.1)	200
	Secure VTY Access Example (5.3.2)	200
	Verify the VTY Port Is Secured (5.3.3)	202
	Configure Extended IPv4 ACLs (5.4)	203
	Extended ACLs (5.4.1)	203
	Numbered Extended IPv4 ACL Syntax (5.4.2)	204
	Protocols and Ports (5.4.3)	206
	<i>Protocol Options</i>	206
	<i>Port Keyword Options</i>	207
	Protocols and Port Numbers Configuration Examples (5.4.4)	208
	Apply a Numbered Extended IPv4 ACL (5.4.5)	209
	TCP Established Extended ACL (5.4.6)	210
	Named Extended IPv4 ACL Syntax (5.4.7)	212
	Named Extended IPv4 ACL Example (5.4.8)	212
	Edit Extended ACLs (5.4.9)	213

- Another Named Extended IPv4 ACL Example (5.4.10) 214
- Verify Extended ACLs (5.4.11) 216
 - show ip interface* 216
 - show access-lists* 217
 - show running-config* 218

Summary (5.5) 219

- Configure Standard IPv4 ACLs 219
- Modify IPv4 ACLs 219
- Secure VTY Ports with a Standard IPv4 ACL 220
- Configure Extended IPv4 ACLs 220

Practice 221

Check Your Understanding Questions 222

Chapter 6

NAT for IPv4 225

Objectives 225

Key Terms 225

Introduction (6.0) 226

NAT Characteristics (6.1) 226

- IPv4 Private Address Space (6.1.1) 226
- What Is NAT? (6.1.2) 227
- How NAT Works (6.1.3) 228
- NAT Terminology (6.1.4) 229
 - Inside Local* 230
 - Inside Global* 230
 - Outside Global* 231
 - Outside Local* 231

Types of NAT (6.2) 231

- Static NAT (6.2.1) 231
- Dynamic NAT (6.2.2) 232
- Port Address Translation (6.2.3) 233
- Next Available Port (6.2.4) 235
- NAT and PAT Comparison (6.2.5) 236
 - NAT* 236
 - PAT* 237
- Packets Without a Layer 4 Segment (6.2.6) 237

NAT Advantages and Disadvantages (6.3) 238

- Advantages of NAT (6.3.1) 238
- Disadvantages of NAT (6.3.2) 238

Static NAT (6.4) 239

- Static NAT Scenario (6.4.1) 240
- Configure Static NAT (6.4.2) 240
- Analyze Static NAT (6.4.3) 241
- Verify Static NAT (6.4.4) 242

Dynamic NAT (6.5) 244

- Dynamic NAT Scenario (6.5.1) 244
- Configure Dynamic NAT (6.5.2) 245
- Analyze Dynamic NAT—Inside to Outside (6.5.3) 247
- Analyze Dynamic NAT—Outside to Inside (6.5.4) 248
- Verify Dynamic NAT (6.5.5) 249

PAT (6.6) 251

- PAT Scenario (6.6.1) 251
- Configure PAT to Use a Single IPv4 Address (6.6.2) 252
- Configure PAT to Use an Address Pool (6.6.3) 253
- Analyze PAT—PC to Server (6.6.4) 254
- Analyze PAT—Server to PC (6.6.5) 255
- Verify PAT (6.6.6) 256

NAT64 (6.7) 258

- NAT for IPv6? (6.7.1) 258
- NAT64 (6.7.2) 258

Summary (6.8) 260

- NAT Characteristics 260
- Types of NAT 260
- NAT Advantages and Disadvantages 261
- Static NAT 261
- Dynamic NAT 262
- PAT 262
- NAT64 263

Practice 264**Check Your Understanding Questions 264****Chapter 7****WAN Concepts 269****Objectives 269****Key Terms 269****Introduction (7.0) 272**

Purpose of WANs (7.1) 272

- LANs and WANs (7.1.1) 272
- Private and Public WANs (7.1.2) 273
- WAN Topologies (7.1.3) 274
 - Point-to-Point Topology* 274
 - Hub-and-Spoke Topology* 275
 - Dual-homed Topology* 276
 - Fully Meshed Topology* 276
 - Partially Meshed Topology* 277
- Carrier Connections (7.1.4) 278
 - Single-Carrier WAN Connection* 278
 - Dual-Carrier WAN Connection* 278
- Evolving Networks (7.1.5) 279
 - Small Network* 279
 - Campus Network* 280
 - Branch Network* 281
 - Distributed Network* 282

WAN Operations (7.2) 283

- WAN Standards (7.2.1) 283
- WANs in the OSI Model (7.2.2) 284
 - Layer 1 Protocols* 284
 - Layer 2 Protocols* 284
- Common WAN Terminology (7.2.3) 285
- WAN Devices (7.2.4) 287
- Serial Communication (7.2.5) 289
- Circuit-Switched Communication (7.2.6) 290
- Packet-Switched Communications (7.2.7) 290
- SDH, SONET, and DWDM (7.2.8) 291

Traditional WAN Connectivity (7.3) 292

- Traditional WAN Connectivity Options (7.3.1) 293
- Common WAN Terminology (7.3.2) 293
- Circuit-Switched Options (7.3.3) 295
 - Public Service Telephone Network (PSTN)* 295
 - Integrated Services Digital Network (ISDN)* 295
- Packet-Switched Options (7.3.4) 295
 - Frame Relay* 295
 - Asynchronous Transfer Mode (ATM)* 296

Modern WAN Connectivity (7.4) 296

Modern WANs (7.4.1) 296

Modern WAN Connectivity Options (7.4.2) 297

Dedicated Broadband 297*Packet-Switched* 298*Internet-Based Broadband* 298

Ethernet WAN (7.4.3) 298

MPLS (7.4.4) 300

Internet-Based Connectivity (7.5) 301

Internet-Based Connectivity Options (7.5.1) 301

Wired Options 302*Wireless Options* 302

DSL Technology (7.5.2) 302

DSL Connections (7.5.3) 303

DSL and PPP (7.5.4) 303

Host with PPPoE Client 304*Router PPPoE Client* 304

Cable Technology (7.5.5) 305

Optical Fiber (7.5.6) 305

Wireless Internet-Based Broadband (7.5.7) 306

Municipal Wi-Fi 306*Cellular* 306*Satellite Internet* 307*WiMAX* 307

VPN Technology (7.5.8) 308

ISP Connectivity Options (7.5.9) 309

Single-Homed 309*Dual-Homed* 309*Multihomed* 309*Dual-Multihomed* 310

Broadband Solution Comparison (7.5.10) 311

Summary (7.6) 312

Purpose of WANs 312

WAN Operations 312

Traditional WAN Connectivity 313

Modern WAN Connectivity 314

Internet-Based Connectivity 314

Practice 315**Check Your Understanding Questions 316**

Chapter 8 VPN and IPsec Concepts 319

Objectives 319

Key Terms 319

Introduction (8.0) 321

VPN Technology (8.1) 321

Virtual Private Networks (8.1.1) 321

VPN Benefits (8.1.2) 322

Site-to-Site and Remote-Access VPNs (8.1.3) 323

Site-to-Site VPN 323

Remote-Access VPN 324

Enterprise and Service Provider VPNs (8.1.4) 324

Types of VPNs (8.2) 325

Remote-Access VPNs (8.2.1) 325

SSL VPNs (8.2.2) 326

Site-to-Site IPsec VPNs (8.2.3) 327

GRE over IPsec (8.2.4) 328

Dynamic Multipoint VPNs (8.2.5) 330

IPsec Virtual Tunnel Interface (8.2.6) 331

Service Provider MPLS VPNs (8.2.7) 332

IPsec (8.3) 333

IPsec Technologies (8.3.2) 333

IPsec Protocol Encapsulation (8.3.3) 336

Confidentiality (8.3.4) 336

Integrity (8.3.5) 338

Authentication (8.3.6) 339

Secure Key Exchange with Diffie-Hellman (8.3.7) 342

Summary (8.4) 344

VPN Technology 344

Types of VPNs 344

IPsec 344

Practice 345

Check Your Understanding Questions 345

Chapter 9 QoS Concepts 351

Objectives 351

Key Terms 351

Introduction (9.0) 353**Network Transmission Quality (9.1) 353**

- Prioritizing Traffic (9.1.2) 353
- Bandwidth, Congestion, Delay, and Jitter (9.1.3) 354
- Packet Loss (9.1.4) 355

Traffic Characteristics (9.2) 357

- Network Traffic Trends (9.2.2) 357
- Voice (9.2.3) 358
- Video (9.2.4) 358
- Data (9.2.5) 360

Queuing Algorithms (9.3) 361

- Queuing Overview (9.3.2) 361
- First-In, First Out (9.3.3) 362
- Weighted Fair Queuing (WFQ) (9.3.4) 362
 - Limitations of WFQ* 363
- Class-Based Weighted Fair Queuing (CBWFQ) (9.3.5) 364
- Low Latency Queuing (LLQ) (9.3.6) 365

QoS Models (9.4) 366

- Selecting an Appropriate QoS Policy Model (9.4.2) 366
- Best Effort (9.4.3) 366
- Integrated Services (9.4.4) 367
- Differentiated Services (9.4.5) 369

QoS Implementation Techniques (9.5) 370

- Avoiding Packet Loss (9.5.2) 371
- QoS Tools (9.5.3) 371
- Classification and Marking (9.5.4) 372
- Marking at Layer 2 (9.5.5) 373
- Marking at Layer 3 (9.5.6) 374
- Type of Service and Traffic Class Field (9.5.7) 375
- DSCP Values (9.5.8) 376
- Class Selector Bits (9.5.9) 377
- Trust Boundaries (9.5.10) 378
- Congestion Avoidance (9.5.11) 379
- Shaping and Policing (9.5.12) 380
- QoS Policy Guidelines (9.5.13) 381

Summary (9.6) 382

- Network Transmission Quality 382
- Traffic Characteristics 382
- Queuing Algorithms 383
- QoS Models 383
- QoS Implementation Techniques 384

Practice 385

Check Your Understanding Questions 385

Chapter 10 Network Management 389

Objectives 389

Key Terms 389

Introduction (10.0) 390

Device Discovery with CDP (10.1) 390

- CDP Overview (10.1.1) 390
- Configure and Verify CDP (10.1.2) 391
- Discover Devices by Using CDP (10.1.3) 393

Device Discovery with LLDP (10.2) 396

- LLDP Overview (10.2.1) 396
- Configure and Verify LLDP (10.2.2) 397
- Discover Devices by Using LLDP (10.2.3) 397

NTP (10.3) 400

- Time and Calendar Services (10.3.1) 400
- NTP Operation (10.3.2) 401
 - Stratum 0* 402
 - Stratum 1* 402
 - Stratum 2 and Lower* 402
- Configure and Verify NTP (10.3.3) 402

SNMP 405

- Introduction to SNMP (10.4.1) 405
- SNMP Operation (10.4.2) 406
- SNMP Agent Traps (10.4.3) 408
- SNMP Versions (10.4.4) 409
- Community Strings (10.4.6) 412
- MIB Object ID (10.4.7) 415
- SNMP Polling Scenario (10.4.8) 415
- SNMP Object Navigator (10.4.9) 417

Syslog (10.5) 418

- Introduction to Syslog (10.5.1) 418
- Syslog Operation (10.5.2) 420
- Syslog Message Format (10.5.3) 421
- Syslog Facilities (10.5.4) 422
- Configure Syslog Timestamp (10.5.5) 422

Router and Switch File Maintenance (10.6) 423

- Router File Systems (10.6.1) 424
 - The Flash File System* 425
 - The NVRAM File System* 425
- Switch File Systems (10.6.2) 426
- Use a Text File to Back Up a Configuration (10.6.3) 427
- Use a Text File to Restore a Configuration (10.6.4) 428
- Use TFTP to Back Up and Restore a Configuration (10.6.5) 428
- USB Ports on a Cisco Router (10.6.6) 430
- Use USB to Back Up and Restore a Configuration (10.6.7) 430
 - Restore Configurations with a USB Flash Drive* 432
- Password Recovery Procedures (10.6.8) 433
- Password Recovery Example (10.6.9) 433
 - Step 1. Enter the ROMMON mode* 433
 - Step 2. Change the configuration register* 434
 - Step 3. Copy the startup-config to the running-config* 434
 - Step 4. Change the password* 435
 - Step 5. Save the running-config as the new startup-config* 435
 - Step 6. Reload the device* 435

IOS Image Management 437

- TFTP Servers as a Backup Location (10.7.2) 437
- Backup IOS Image to TFTP Server Example (10.7.3) 438
 - Step 1. Ping the TFTP server* 438
 - Step 2. Verify image size in flash* 439
 - Step 3. Copy the image to the TFTP server* 439
- Copy an IOS Image to a Device Example (10.7.4) 439
 - Step 1. Ping the TFTP server* 440
 - Step 2. Verify the amount of free flash* 440
 - Step 3. Copy the new IOS image to flash* 441
- The boot system Command (10.7.5) 441

Summary (10.8) 443

- Device Discovery with CDP 443
- Device Discovery with LLDP 443

- NTP 443
- SNMP 444
- Syslog 444
- Router and Switch File Maintenance 445
- IOS Image Management 446

Practice 446

Check Your Understanding Questions 447

Chapter 11 Network Design 453

Objectives 453

Key Terms 453

Introduction (11.0) 455

Hierarchical Networks (11.1) 455

- The Need to Scale the Network (11.1.2) 455
- Borderless Switched Networks (11.1.3) 458
- Hierarchy in the Borderless Switched Network (11.1.4) 459
 - Three-Tier Model* 460
 - Two-Tier Model* 461
- Access, Distribution, and Core Layer Functions (11.1.5) 462
 - Access Layer* 462
 - Distribution Layer* 462
 - Core Layer* 462
- Three-Tier and Two-Tier Examples (11.1.6) 462
 - Three-Tier Example* 463
 - Two-Tier Example* 464
- Role of Switched Networks (11.1.7) 464

Scalable Networks (11.2) 465

- Design for Scalability (11.2.1) 465
 - Redundant Links* 466
 - Multiple Links* 466
 - Scalable Routing Protocol* 467
 - Wireless Connectivity* 468
- Plan for Redundancy (11.2.2) 469
- Reduce Failure Domain Size (11.2.3) 470
 - Edge Router* 470
 - API* 471
 - S1* 472

S2	472
S3	473
<i>Limiting the Size of Failure Domains</i>	474
<i>Switch Block Deployment</i>	474
Increase Bandwidth (11.2.4)	474
Expand the Access Layer (11.2.5)	475
Tune Routing Protocols (11.2.6)	476
Switch Hardware (11.3)	477
Switch Platforms (11.3.1)	477
<i>Campus LAN Switches</i>	477
<i>Cloud-Managed Switches</i>	478
<i>Data Center Switches</i>	478
<i>Service Provider Switches</i>	479
<i>Virtual Networking</i>	479
Switch Form Factors (11.3.2)	479
<i>Fixed Configuration Switches</i>	480
<i>Modular Configuration Switches</i>	480
<i>Stackable Configuration Switches</i>	481
<i>Thickness</i>	481
Port Density (11.3.3)	482
Forwarding Rates (11.3.4)	483
Power over Ethernet (11.3.5)	484
<i>Switch</i>	484
<i>IP Phone</i>	484
WAP	485
<i>Cisco Catalyst 2960-C</i>	485
Multilayer Switching (11.3.6)	485
Business Considerations for Switch Selection (11.3.7)	486
Router Hardware (11.4)	487
Router Requirements (11.4.1)	487
Cisco Routers (11.4.2)	488
<i>Branch Routers</i>	488
<i>Network Edge Routers</i>	488
<i>Service Provider Routers</i>	489
<i>Industrial</i>	490
Router Form Factors (11.4.3)	490
<i>Cisco 900 Series</i>	490
<i>ASR 9000 and 1000 Series</i>	490
<i>5500 Series</i>	491
<i>Cisco 800</i>	492
<i>Fixed Configuration or Modular</i>	492

Summary (11.5) 493

Hierarchical Networks 493

Scalable Networks 493

Switch Hardware 494

Router Hardware 494

Practice 495

Check Your Understanding Questions 496

Chapter 12 Network Troubleshooting 501

Objectives 501

Key Terms 501

Introduction (12.0) 502

Network Documentation (12.1) 502

Documentation Overview (12.1.1) 502

Network Topology Diagrams (12.1.2) 503

Physical Topology 503

Logical IPv4 Topology 504

Logical IPv6 Topology 505

Network Device Documentation (12.1.3) 505

Router Device Documentation 505

LAN Switch Device Documentation 506

End-System Documentation Files 506

Establish a Network Baseline (12.1.4) 507

Step 1—Determine What Types of Data to Collect (12.1.5) 508

Step 2—Identify Devices and Ports of Interest (12.1.6) 508

Step 3—Determine the Baseline Duration (12.1.7) 509

Data Measurement (12.1.8) 510

Troubleshooting Process (12.2) 512

General Troubleshooting Procedures (12.2.1) 512

Seven-Step Troubleshooting Process (12.2.2) 513

Define the Problem 514

Gather Information 514

Analyze Information 514

Eliminate Possible Causes 514

Propose Hypothesis 514

Test Hypothesis 515

Solve the Problem 515

Question End Users (12.2.3) 515

Gather Information (12.2.4)	516
Troubleshooting with Layered Models (12.2.5)	517
Structured Troubleshooting Methods (12.2.6)	518
<i>Bottom-Up</i>	518
<i>Top-Down</i>	519
<i>Divide-and-Conquer</i>	520
<i>Follow-the-Path</i>	521
<i>Substitution</i>	522
<i>Comparison</i>	522
<i>Educated Guess</i>	522
Guidelines for Selecting a Troubleshooting Method (12.2.7)	523
Troubleshooting Tools (12.3)	524
Software Troubleshooting Tools (12.3.1)	524
<i>Network Management System Tools</i>	524
<i>Knowledge Bases</i>	524
<i>Baselining Tools</i>	524
Protocol Analyzers (12.3.2)	525
Hardware Troubleshooting Tools (12.3.3)	525
<i>Digital Multimeters</i>	525
<i>Cable Testers</i>	526
<i>Cable Analyzers</i>	527
<i>Portable Network Analyzers</i>	528
<i>Cisco Prime NAM</i>	528
Syslog Server as a Troubleshooting Tool (12.3.4)	529
Symptoms and Causes of Network Problems (12.4)	531
Physical Layer Troubleshooting (12.4.1)	531
Data Link Layer Troubleshooting (12.4.2)	534
Network Layer Troubleshooting (12.4.3)	537
Transport Layer Troubleshooting—ACLs (12.4.4)	539
Transport Layer Troubleshooting—NAT for IPv4 (12.4.5)	542
Application Layer Troubleshooting (12.4.6)	543
Troubleshooting IP Connectivity (12.5)	545
Components of Troubleshooting End-to-End Connectivity (12.5.1)	545
End-to-End Connectivity Problem Initiates Troubleshooting (12.5.2)	547
<i>IPv4 ping</i>	547
<i>IPv4 traceroute</i>	548
<i>IPv6 ping and traceroute</i>	548

Step 1—Verify the Physical Layer (12.5.3)	549
<i>Input Queue Drops</i>	550
<i>Output Queue Drops</i>	550
<i>Input Errors</i>	551
<i>Output Errors</i>	551
Step 2—Check for Duplex Mismatches (12.5.4)	551
<i>Troubleshooting Example</i>	552
Step 3—Verify Addressing on the Local Network (12.5.5)	553
<i>Windows IPv4 ARP Table</i>	553
<i>Windows IPv6 Neighbor Table</i>	554
<i>IOS IPv6 Neighbor Table</i>	555
<i>Switch MAC Address Table</i>	555
Troubleshoot VLAN Assignment Example (12.5.6)	556
<i>Check the ARP Table</i>	557
<i>Check the Switch MAC Table</i>	557
<i>Correct the VLAN Assignment</i>	557
Step 4—Verify Default Gateway (12.5.7)	558
<i>Troubleshooting IPv4 Default Gateway Example</i>	559
<i>R1 Routing Table</i>	559
<i>PC1 Routing Table</i>	559
Troubleshoot IPv6 Default Gateway Example (12.5.8)	560
<i>R1 Routing Table</i>	560
<i>PC1 Addressing</i>	560
<i>Check R1 Interface Settings</i>	561
<i>Correct R1 IPv6 Routing</i>	561
<i>Verify PC1 Has an IPv6 Default Gateway</i>	562
Step 5—Verify Correct Path (12.5.9)	562
<i>Troubleshooting Example</i>	566
Step 6—Verify the Transport Layer (12.5.10)	566
<i>Troubleshooting Example</i>	566
Step 7—Verify ACLs (12.5.11)	568
<i>Troubleshooting Example</i>	568
<i>show ip access-lists</i>	569
<i>show ip interfaces</i>	569
<i>Correct the Issue</i>	570
Step 8—Verify DNS (12.5.12)	570
Summary (12.6)	572
Network Documentation	572
Troubleshooting Process	572
Troubleshooting Tools	573

	Symptoms and Causes of Network Problems	573
	Troubleshooting IP Connectivity	574
	Practice	577
	Check Your Understanding Questions	577
Chapter 13	Network Virtualization	581
	Objectives	581
	Key Terms	581
	Introduction (13.0)	583
	Cloud Computing (13.1)	583
	Cloud Overview (13.1.2)	583
	Cloud Services (13.1.3)	584
	Cloud Models (13.1.4)	584
	Cloud Computing Versus Data Center (13.1.5)	585
	Virtualization (13.2)	585
	Cloud Computing and Virtualization (13.2.1)	585
	Dedicated Servers (13.2.2)	586
	Server Virtualization (13.2.3)	587
	Advantages of Virtualization (13.2.4)	589
	Abstraction Layers (13.2.5)	589
	Type 2 Hypervisors (13.2.6)	591
	Virtual Network Infrastructure (13.3)	592
	Type 1 Hypervisors (13.3.1)	592
	Installing a VM on a Hypervisor (13.3.2)	592
	The Complexity of Network Virtualization (13.3.3)	594
	Software-Defined Networking (13.4)	595
	Control Plane and Data Plane (13.4.2)	595
	<i>Layer 3 Switch and CEF</i>	596
	<i>SDN and Central Controller</i>	597
	<i>Management Plane</i>	598
	Network Virtualization Technologies (13.4.3)	598
	Traditional and SDN Architectures (13.4.4)	599
	Controllers (13.5)	600
	SDN Controller and Operations (13.5.1)	600
	Core Components of ACI (13.5.3)	602
	Spine-Leaf Topology (13.5.4)	603

- SDN Types (13.5.5) 604
 - Device-Based SDN* 604
 - Controller-Based SDN* 605
 - Policy-Based SDN* 605
- APIC-EM Features (13.5.6) 606
- APIC-EM Path Trace (13.5.7) 606

Summary (13.6) 609

- Cloud Computing 609
- Virtualization 609
- Virtual Network Infrastructure 610
- Software-Defined Networking 610
- Controllers 611

Practice 612

Check Your Understanding Questions 613

Chapter 14 Network Automation 617

Objectives 617

Key Terms 617

Introduction (14.0) 619

Automation Overview (14.1) 619

- The Increase in Automation (14.1.2) 619
- Thinking Devices (14.1.3) 620

Data Formats (14.2) 620

- The Data Formats Concept (14.2.2) 620
- Data Format Rules (14.2.3) 622
- Compare Data Formats (14.2.4) 623
- JSON Data Format (14.2.5) 624
- JSON Syntax Rules (14.2.6) 624
- YAML Data Format (14.2.7) 626
- XML Data Format (14.2.8) 627

APIs (14.3) 628

- The API Concept (14.3.2) 628
- An API Example (14.3.3) 629
- Open, Internal, and Partner APIs (14.3.4) 631
- Types of Web Service APIs (14.3.5) 632

REST (14.4) 633

- REST and RESTful API (14.4.2) 633
- RESTful Implementation (14.4.3) 634
- URI, URN, and URL (14.4.4) 635
- Anatomy of a RESTful Request (14.4.5) 636
- RESTful API Applications (14.4.6) 638
 - Developer Website* 638
 - Postman* 638
 - Python* 638
 - Network Operating Systems* 638

Configuration Management Tools (14.5) 639

- Traditional Network Configuration (14.5.2) 639
- Network Automation (14.5.3) 641
- Configuration Management Tools (14.5.4) 642
- Compare Ansible, Chef, Puppet, and SaltStack (14.5.5) 642

IBN and Cisco DNA Center (14.6) 644

- Intent-Based Networking Overview (14.6.2) 644
- Network Infrastructure as Fabric (14.6.3) 644
- Cisco Digital Network Architecture (DNA) (14.6.4) 647
- Cisco DNA Center (14.6.5) 648

Summary (14.7) 651

- Automation Overview 651
- Data Formats 651
- APIs 651
- REST 651
- Configuration and Management 652
- IBN and Cisco DNA Center 652

Practice 652**Check Your Understanding Questions 653****Appendix A Answers to the “Check Your Understanding” Questions 657****Glossary 677****Index 715**

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

Enterprise Networking, Security, and Automation Companion Guide (CCNAv7) is the official supplemental textbook for the Cisco Network Academy CCNA Enterprise Networking, Security, and Automation version 7 course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application and provides opportunities to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small to medium-sized businesses as well as enterprise and service provider environments.

This book provides a ready reference that explains the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternative explanations and examples to supplement the course. You can use the online curriculum as directed by your instructor and then use this *Companion Guide*'s study tools to help solidify your understanding of all the topics.

Who Should Read This Book

The book, like the course it accompanies, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Networking Academy courses and preparation for the CCNA certification.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following list gives you a thorough overview of the features provided in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives listed in the corresponding chapters of the online curriculum; however, the question

format in the *Companion Guide* encourages you to think about finding the answers as you read the chapter.

- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Summary:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of each chapter is a full list of all the labs, class activities, and Packet Tracer activities to refer to at study time.

Readability

The following features are provided to help you understand networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference to find the term used inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary that defines more than 1000 terms.

Practice

Practice makes perfect. This *Companion Guide* offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key:** Review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions in the online course. Appendix A, “Answers to the Check Your Understanding Questions,” provides an answer key to all the questions and includes an explanation of each answer.
- **Labs and activities:** Throughout each chapter, you are directed back to the online course to take advantage of the activities provided to reinforce concepts. In addition, at the end of each chapter is a “Practice” section that lists all the labs and activities to provide practice with the topics introduced in this chapter.
- **Page references to online course:** After most headings is a number in parentheses—for example, (1.1.2). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.



Interactive
Graphic

Video

About Packet Tracer Software and Activities

Interspersed throughout the chapters, you'll find a few Cisco Packet Tracer activities. Packet Tracer allows you to create networks, visualize how packets flow in a network, and use basic testing tools to determine whether a network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the online course. Packet Tracer software is available only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Enterprise Networking, Security, and Automation v7 course and is divided into 14 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, “Single-Area OSPFv2 Concepts”:** This chapter explains single-area OSPF. It describes basic OSPF features and characteristics, packet types, and single-area operation.
- **Chapter 2, “Single-Area OSPFv2 Configuration”:** This chapter explains 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 a single-area OSPFv2 configuration.
- **Chapter 3, “Network Security Concepts”:** This chapter explains 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 explains how ACLs are used to filter traffic, how wildcard masks are used, how to create ACLs, and the difference between standard and extended IPv4 ACLs.
- **Chapter 5, “ACLs for IPv4 Configuration”:** The chapter explains 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 explains 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 explains 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 explains 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 explains how network devices use QoS to prioritize network traffic. It includes descriptions of network transmission characteristics, queuing algorithms, different queuing models, and QoS implementation techniques.
- **Chapter 10, “Network Management”:** This chapter explains how to use a variety of protocols and techniques to manage a 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 explains 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 describes how to troubleshoot networks. It includes explanations of network documentation, troubleshooting methods, and troubleshooting tools. The chapter also demonstrates how to troubleshoot symptoms and causes of network problems using a layered approach.
- **Chapter 13, “Network Virtualization”:** This chapter describes 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 explains network automation. It includes descriptions of automation, data formats, APIs, REST, configuration management tools, and Cisco DNA Center.
- **Appendix A, “Answers to the ‘Check Your Understanding’ Questions”:** This appendix lists the answers to the questions in the “Check Your Understanding Questions” section at the end of each chapter.
- **Glossary:** The Glossary provides definitions for all the key terms identified in each chapter.

Figure Credits

Figure 5-4, screenshot of Remote Access from PC1 © Tera Term Project

Figure 5-5, screenshot of Remote Access Attempt from PC2 © Tera Term Project

Figure 8-9, screenshot of Wireshark of Encapsulated Protocols © Wireshark

Figure 10-24, screenshot of Example of Using Tera Term to Backup a Configuration © Tera Term Project

Figure 10-25, screenshot of Example of Using Tera Term to Send a Configuration © Tera Term Project

Figure 12-16, screenshot of Wireshark Capture © Wireshark

Figure 13-1, screenshot of AWS Management Console © 2020, Amazon Web Services, Inc

Figure 14-1, screenshot of HTML Example and Resulting Web Page © WHATWG

This page intentionally left blank

ACL Concepts

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- How do ACLs filter traffic?
- How do ACLs use wildcard masks?
- How do you create ACLs?
- What are the differences between standard and extended IPv4 ACLs?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

access control entry (ACE) page 164

inbound ACL page 167

outbound ACL page 167

implicit deny page 167

wildcard mask page 168

numbered ACL page 175

standard ACL page 175

extended ACL page 175

named ACL page 176

Introduction (4.0)

Say that you have arrived at your grandparents' residence. It is a beautiful gated community with walking paths and gardens. For the safety of the residents, no one is permitted to get into the community without stopping at the gate and presenting the guard with identification. You provide your ID, and the guard verifies that you are expected as a visitor. He documents your information and lifts the gate. Imagine if the guard had to do this for the many staff members who entered each day. The security department has simplified this process by assigning a badge to each employee that can be scanned to automatically raise the gate. You greet your grandparents, who are anxiously awaiting you at the front desk. You all get back into the car to go down the street for dinner. As you exit the parking lot, you must again stop and show your identification so that the guard will lift the gate. Rules have been put in place for all incoming and outgoing traffic.

Much like the guard in the gated community, an access control list (ACL) may be configured to permit and deny network traffic passing through an interface. The router compares the information within a packet against each access control entry (ACE), in sequential order, to determine if the packet matches one of the ACEs. This process is called *packet filtering*. Let's learn more!

Purpose of ACLs (4.1)

This section describes how ACLs filter traffic in small- to medium-sized business networks.

What Is an ACL? (4.1.1)

Routers make routing decisions based on information in each packet's header. Traffic entering a router interface is routed solely based on information in the routing table. The router compares the destination IP address with routes in the routing table to find the best match and then forwards a packet based on the best match route. A similar process can be used to filter traffic using an access control list (ACL).

An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. By default, a router does not have any ACLs configured. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine if each packet can be forwarded.

An ACL uses a sequential list of permit or deny statements known as *access control entries (ACEs)*.

Note

ACEs are also commonly called ACL statements.

When network traffic passes through an interface configured with an ACL, the router compares the information within the packet against each ACE, in sequential order, to determine whether the packet matches one of the ACEs. This process is called packet *filtering*.

Several tasks performed by routers require the use of ACLs to identify traffic. Table 4-1 lists some of these tasks and provides examples.

Table 4-1 Tasks That Use ACLs

Task	Example
Limit network traffic to increase network performance	<ul style="list-style-type: none"> ■ A corporate policy prohibits video traffic on the network to reduce the network load. ■ A policy can be enforced using ACLs to block video traffic.
Provide traffic flow control	<ul style="list-style-type: none"> ■ A corporate policy requires that routing protocol traffic be limited to certain links only. ■ A policy can be implemented using ACLs to restrict the delivery of routing updates to only those that come from a known source.
Provide a basic level of security for network access	<ul style="list-style-type: none"> ■ Corporate policy demands that access to the human resources network be restricted to authorized users only. ■ A policy can be enforced using ACLs to limit access to specified networks.
Filter traffic based on traffic type	<ul style="list-style-type: none"> ■ Corporate policy requires that email traffic be permitted into a network but that Telnet access be denied. ■ A policy can be implemented using ACLs to filter traffic by type.
Screen hosts to permit or deny access to network services	<ul style="list-style-type: none"> ■ Corporate policy requires that access to some file types (such as FTP or HTTP) be limited to user groups. ■ A policy can be implemented using ACLs to filter user access to services.
Provide priority to certain classes of network traffic	<ul style="list-style-type: none"> ■ Corporate traffic specifies that voice traffic be forwarded as fast as possible to avoid any interruption. ■ A policy can be implemented using ACLs and QoS to identify voice traffic and process it immediately.

Packet Filtering (4.1.2)

Packet filtering controls access to a network by analyzing the incoming and/or outgoing packets and forwarding them or discarding them based on given criteria. Packet filtering can occur at Layer 3 or Layer 4, as shown in Figure 4-1.

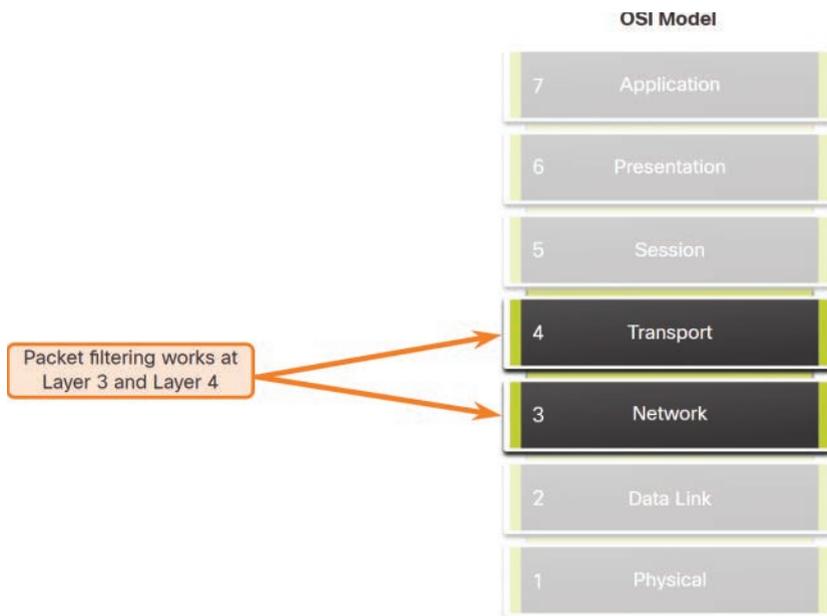


Figure 4-1 Packet Filtering in the OSI Model

Cisco routers support two types of ACLs:

- **Standard ACLs:** These ACLs only filter at Layer 3, using the source IPv4 address only.
- **Extended ACLs:** These ACLs filter at Layer 3 using the source and/or destination IPv4 address. They can also filter at Layer 4 using TCP, UDP ports, and optional protocol type information for finer control.

ACL Operation (4.1.3)

An ACL defines a set of rules that give added control for packets that enter inbound interfaces, packets relayed through the router, and packets that exit outbound interfaces of the router.

ACLs can be configured to apply to inbound traffic and outbound traffic, as shown in Figure 4-2.



Figure 4-2 ACLs on Inbound and Outbound Interfaces

Note

ACLs do not act on packets that originate from the router itself.

An *inbound ACL* filters packets before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If a packet is permitted by the ACL, it is processed for routing. Inbound ACLs are best used to filter packets when the network attached to an inbound interface is the only source of packets that need to be examined.

An *outbound ACL* filters packets after they are routed, regardless of the inbound interface. Incoming packets are routed to the outbound interface, and they are then processed through the outbound ACL. Outbound ACLs are best used when the same filter will be applied to packets coming from multiple inbound interfaces before exiting the same outbound interface.

When an ACL is applied to an interface, it follows a specific operating procedure. For example, here are the operational steps used when traffic has entered a router interface with an inbound standard IPv4 ACL configured:

- Step 1.** The router extracts the source IPv4 address from the packet header.
- Step 2.** The router starts at the top of the ACL and compares the source IPv4 address to each ACE, in sequential order.
- Step 3.** When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
- Step 4.** If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an *implicit deny* ACE automatically applied to all ACLs.

The last ACE statement of an ACL is always an implicit deny that blocks all traffic. By default, this statement is automatically implied at the end of an ACL even though it is hidden and not displayed in the configuration.

Note

An ACL must have at least one permit statement; otherwise, all traffic will be denied due to the implicit deny ACE statement.

**Packet Tracer—ACL Demonstration (4.1.4)**

In this activity, you will observe how an ACL can be used to prevent a ping from reaching hosts on remote networks. After removing the ACL from the configuration, the pings will be successful.

Interactive
Graphic**Check Your Understanding—Purpose of ACLs (4.1.5)**

Refer to the online course to complete this activity.

Wildcard Masks in ACLs (4.2)

A wildcard mask is similar to a subnet mask but the reverse. In this section, you will learn how to calculate the inverse wildcard mask.

Wildcard Mask Overview (4.2.1)

In the previous section, you learned about the purpose of ACL. This section explains how ACLs use *wildcard masks*. An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match. Wildcard masks are also used by the Open Shortest Path First (OSPF) routing protocol.

A wildcard mask is similar to a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match. However, a wildcard mask and a subnet mask differ in the way they match binary 1s and 0s. Unlike with a subnet mask, in which binary 1 is equal to a match, and binary 0 is not a match, with a wildcard mask, the reverse is true.

Wildcard masks use the following rules to match binary 1s and 0s:

- **Wildcard mask bit 0:** Match the corresponding bit value in the address.
- **Wildcard mask bit 1:** Ignore the corresponding bit value in the address.

Table 4-2 lists some examples of wildcard masks and what they would match and ignore.

Table 4-2 Examples of Wildcard Masks

Wildcard Mask	Last Octet (in Binary)	Meaning (0—match, 1—ignore)
0.0.0.0	00000000	<ul style="list-style-type: none"> ■ Match all octets.
0.0.0.63	00111111	<ul style="list-style-type: none"> ■ Match the first three octets ■ Match the 2 leftmost bits of the last octet ■ Ignore the last 6 bits
0.0.0.15	00001111	<ul style="list-style-type: none"> ■ Match the first three octets ■ Match the 4 leftmost bits of the last octet ■ Ignore the last 4 bits of the last octet

Wildcard Mask	Last Octet (in Binary)	Meaning (0—match, 1—ignore)
0.0.0.248	11111100	<ul style="list-style-type: none"> ■ Match the first three octets ■ Ignore the 6 leftmost bits of the last octet ■ Match the last 2 bits
0.0.0.255	11111111	<ul style="list-style-type: none"> ■ Match the first three octets ■ Ignore the last octet

Wildcard Mask Types (4.2.2)

Using wildcard masks takes some practice. The following sections provide examples to help you learn how wildcard masks are used to filter traffic for one host, one subnet, and a range IPv4 addresses.

Wildcard to Match a Host

In this example, the wildcard mask is used to match a specific host IPv4 address. Say that ACL 10 needs an ACE that only permits the host with IPv4 address 192.168.1.1. Recall that 0 equals a match, and 1 equals ignore. To match a specific host IPv4 address, a wildcard mask consisting of all zeros (that is, 0.0.0.0) is required.

Table 4-3 lists, in decimal and binary, the host IPv4 address, the wildcard mask, and the permitted IPv4 address.

Table 4-3 Wildcard to Match a Host Example

	Decimal	Binary
IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard mask	0.0.0.0	00000000.00000000.00000000.00000000
Permitted IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001

The 0.0.0.0 wildcard mask stipulates that every bit must match exactly. Therefore, when the ACE is processed, the wildcard mask will permit only the 192.168.1.1 address. The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.1.1 0.0.0.0**.

Wildcard Mask to Match an IPv4 Subnet

In this example, ACL 10 needs an ACE that permits all hosts in the 192.168.1.0/24 network. The wildcard mask 0.0.0.255 stipulates that the very first three octets must match exactly, but the fourth octet does not need to match.

Table 4-4 lists, in decimal and binary, the host IPv4 address, the wildcard mask, and the permitted IPv4 addresses.

Table 4-4 Wildcard Mask to Match an IPv4 Subnet Example

	Decimal	Binary
IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard mask	0.0.0.255	00000000.00000000.00000000.11111111
Permitted IPv4 address	192.168.1.0/24	11000000.10101000.00000000.1.00000000

When the ACE is processed, the wildcard mask 0.0.0.255 permits all hosts in the 192.168.1.0/24 network. The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.1.0 0.0.0.255**.

Wildcard Mask to Match an IPv4 Address Range

In this example, ACL 10 needs an ACE that permits all hosts in the 192.168.16.0/24, 192.168.17.0/24, ..., 192.168.31.0/24 networks. The wildcard mask 0.0.15.255 would correctly filter that range of addresses.

Table 4-5 lists, in decimal and binary the host IPv4 address, the wildcard mask, and the permitted IPv4 addresses.

Table 4-5 Wildcard Mask to Match an IPv4 Address Range Example

	Decimal	Binary
IPv4 address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard mask	0.0.15.255	00000000.00000000.00001111.11111111
Permitted IPv4 address	192.168.16.0/24 to 192.168.31.0/24	11000000.10101000.00010000.00000000 11000000.10101000.00011111.00000000

The highlighted wildcard mask bits identify which bits of the IPv4 address must match. When the ACE is processed, the wildcard mask 0.0.15.255 permits all hosts in the 192.168.16.0/24 to 192.168.31.0/24 networks. The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.16.0 0.0.15.255**.

Wildcard Mask Calculation (4.2.3)

Calculating wildcard masks can be challenging. One shortcut method is to subtract the subnet mask from 255.255.255.255. The following sections provide examples to help you learn how to calculate the wildcard mask using the subnet mask.

Example 1

Say that you wanted an ACE in ACL 10 to permit access to all users in the 192.168.3.0/24 network. To calculate the wildcard mask, subtract the subnet mask (that is, 255.255.255.0) from 255.255.255.255, as shown in Table 4-6.

The solution produces the wildcard mask 0.0.0.255. Therefore, the ACE would be `access-list 10 permit 192.168.3.0 0.0.0.255`.

Table 4-6 Wildcard Mask Calculation—Example 1

Starting value	255.255.255.255
Subtract the subnet mask	-255.255.255. 0
Resulting wildcard mask	0. 0. 0.255

Example 2

In this example, say that you wanted an ACE in ACL 10 to permit network access for the 14 users in the subnet 192.168.3.32/28. Subtract the subnet (that is, 255.255.255.240) from 255.255.255.255, as shown in Table 4-7.

This solution produces the wildcard mask 0.0.0.15. Therefore, the ACE would be `access-list 10 permit 192.168.3.32 0.0.0.15`.

Table 4-7 Wildcard Mask Calculation—Example 2

Starting value	255.255.255.255
Subtract the subnet mask	-255.255.255.240
Resulting wildcard mask	0. 0. 0. 15

Example 3

In this example, say that you needed an ACE in ACL 10 to permit only networks 192.168.10.0 and 192.168.11.0. These two networks could be summarized as 192.168.10.0/23, which is a subnet mask of 255.255.254.0. Again, you subtract 255.255.254.0 subnet mask from 255.255.255.255, as shown in Table 4-8.

This solution produces the wildcard mask 0.0.1.255. Therefore, the ACE would be `access-list 10 permit 192.168.10.0 0.0.1.255`.

Table 4-8 Wildcard Mask Calculation—Example 3

Starting value	255.255.255.255
Subtract the subnet mask	-255.255.254. 0
Resulting wildcard mask	0. 0. 1.255

Example 4

Consider an example in which you need an ACL number 10 to match networks in the range 192.168.16.0/24 to 192.168.31.0/24. This network range could be summarized as 192.168.16.0/20, which is a subnet mask of 255.255.240.0. Therefore, subtract 255.255.240.0 subnet mask from 255.255.255.255, as shown in Table 4-9.

This solution produces the wildcard mask 0.0.15.255. Therefore, the ACE would be `access-list 10 permit 192.168.16.0 0.0.15.255`.

Table 4-9 Wildcard Mask Calculation—Example 4

Starting value	255.255.255.255
Subtract the subnet mask	– 255.255.240. 0
Resulting wildcard mask	0. 0. 15.255

Wildcard Mask Keywords (4.2.4)

Working with decimal representations of binary wildcard mask bits can be tedious. To simplify this task, Cisco IOS provides two keywords to identify the most common uses of wildcard masking. Keywords reduce ACL keystrokes and make it easier to read an ACE.

The two keywords are

- **host:** This keyword substitutes for the 0.0.0.0 mask and indicates that all IPv4 address bits must match to filter just one host address.
- **any:** This keyword substitutes for the 255.255.255.255 mask and indicates to ignore the entire IPv4 address or to accept any addresses.

In the command output in Example 4-1, two ACLs are configured. The ACL 10 ACE permits only the 192.168.10.10 host, and the ACL 11 ACE permits all hosts.

Example 4-1 ACLs Configured Without Keywords

```
R1(config)# access-list 10 permit 192.168.10.10 0.0.0.0
R1(config)# access-list 11 permit 0.0.0.0 255.255.255.255
R1(config)#
```

Alternatively, the keywords **host** and **any** could be used to replace the highlighted output. The commands in Example 4-2 accomplishes the same task as the commands in Example 4-1.

Example 4-2 ACLs Configured Using Keywords

```
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# access-list 11 permit any
R1(config)#
```

**Interactive
Graphic****Check Your Understanding—Wildcard Masks in ACLs (4.2.5)**

Refer to the online course to complete this activity.

Guidelines for ACL Creation (4.3)

This section provides guidelines for creating ACLs.

Limited Number of ACLs per Interface (4.3.1)

In a previous section, you learned about how wildcard masks are used in ACLs. This section discusses guidelines for ACL creation. There is a limit on the number of ACLs that can be applied on a router interface. For example, a dual-stacked (that is, IPv4 and IPv6) router interface can have up to four ACLs applied, as shown in Figure 4-3.

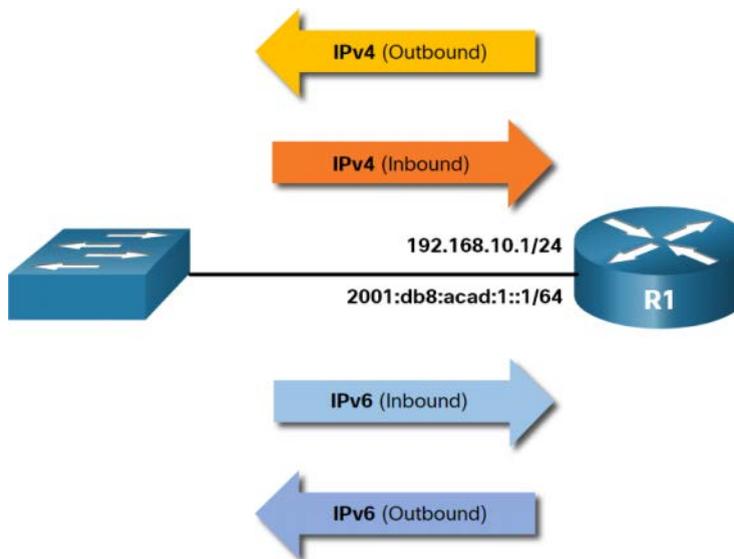


Figure 4-3 ACLs Limited on Interfaces

Specifically, a dual-stacked router interface can have

- One outbound IPv4 ACL
- One inbound IPv4 ACL
- One inbound IPv6 ACL
- One outbound IPv6 ACL

Say that R1 has two dual-stacked interfaces that need to have inbound and outbound IPv4 and IPv6 ACLs applied. As shown in Figure 4-4, R1 could have up to 8 ACLs configured and applied to interfaces.

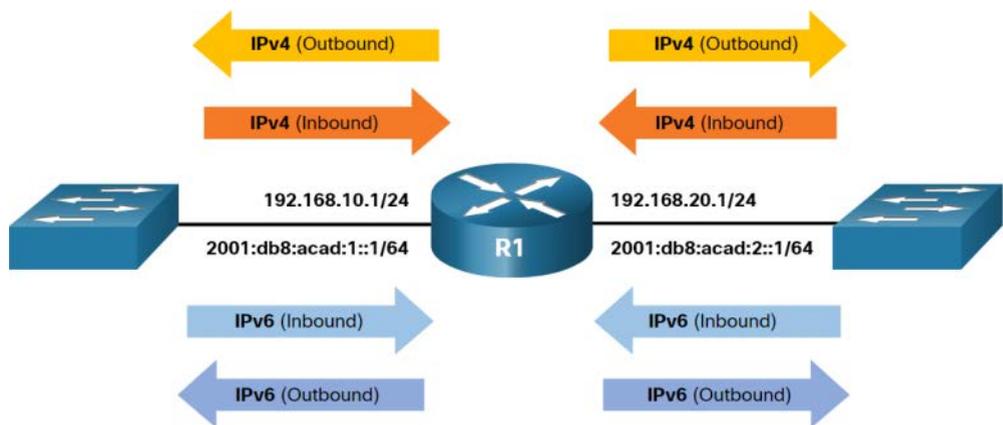


Figure 4-4 ACLs Limit Example

In this case, each interface would have four ACLs: two ACLs for IPv4 and two ACLs for IPv6. For each protocol, one ACL is for inbound traffic and one for outbound traffic.

Note

ACLs do not have to be configured in both directions. The number of ACLs and their direction applied to the interface will depend on the security policy of the organization.

ACL Best Practices (4.3.2)

Using ACLs requires attention to detail and great care. Mistakes can be costly in terms of downtime, troubleshooting efforts, and network service. Basic planning is required before configuring an ACL.

Table 4-10 presents some ACL best practices.

Table 4-10 Guidelines for ACLs

Guideline	Benefit
Base ACLs on the organization's security policies.	This will ensure that you implement organizational security guidelines.
Write out what you want an ACL to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit, and save all your ACLs.	This will help you create a library of reusable ACLs.
Document ACLs by using the remark command.	This will help you (and others) understand the purpose of an ACE.
Test ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

**Interactive
Graphic**
Check Your Understanding—Guidelines for ACL Creation (4.3.3)

Refer to the online course to complete this activity.

Types of IPv4 ACLs (4.4)

This section compares IPv4 standard and extended ACLs.

Standard and Extended ACLs (4.4.1)

The previous sections describe the purpose of ACLs as well as guidelines for ACL creation. This section covers standard and extended ACLs and named and *numbered ACLs*, and it provides examples of placement of these ACLs.

There are two types of IPv4 ACLs:

- **Standard ACLs:** These ACLs permit or deny packets based only on the source IPv4 address.
- **Extended ACLs:** These ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more.

For example, Example 4-3 shows how to create a standard ACL. In this example, ACL 10 permits hosts on the source network 192.168.10.0/24. Because of the implied “deny any” at the end, all traffic except for traffic coming from the 192.168.10.0/24 network is blocked with this ACL.

Example 4-3 Standard ACL Example

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#
```

In Example 4-4, the extended ACL 100 permits traffic originating from any host on the 192.168.10.0/24 network to any IPv4 network if the destination host port is 80 (HTTP).

Example 4-4 Extended ACL Example

```
R1(config)# access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)#
```

Notice that the standard ACL 10 is only capable of filtering by source address, while the extended ACL 100 is filtering on the source and destination Layer 3 and Layer 4 protocol (for example, TCP) information.

Note

Full IPv4 ACL configuration is discussed in Chapter 5, “ACLs for IPv4 Configuration.”

Numbered and Named ACLs (4.4.2)

For IPv4, there are both numbered and *named ACLs*.

Numbered ACLs

ACLs 1 to 99 and 1300 to 1999 are standard ACLs, while ACLs 100 to 199 and 2000 to 2699 are extended ACLs, as shown in Example 4-5.

Example 4-5 Available ACL Numbers

```
R1(config)# access-list ?
  <1-99>          IP standard access list
  <100-199>       IP extended access list
  <1100-1199>     Extended 48-bit MAC address access list
  <1300-1999>    IP standard access list (expanded range)
  <200-299>      Protocol type-code access list
  <2000-2699>    IP extended access list (expanded range)
  <700-799>      48-bit MAC address access list
  rate-limit     Simple rate-limit specific access list
  template       Enable IP template acls
Router(config)# access-list
```

Named ACLs

Using named ACLs is the preferred method when configuring ACLs. You can name standard and extended ACLs to provide information about the purpose of each ACL. For example, the extended ACL name FTP-FILTER is far easier to identify than the ACL number 100.

The `ip access-list` global configuration command is used to create a named ACL, as shown in Example 4-6.

Note

Numbered ACLs are created using the `access-list` global configuration command.

Example 4-6 Example of a Named ACL

```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
R1(config-ext-nacl)#
```

The following are the general rules to follow for named ACLs:

- Assign a name to identify the purpose of the ACL.
- Names can contain alphanumeric characters.
- Names cannot contain spaces or punctuation.
- It is suggested that a name be written in CAPITAL LETTERS.
- Entries can be added or deleted within an ACL.

Where to Place ACLs (4.4.3)

Every ACL should be placed where it has the greatest impact on efficiency.

Figure 4-5 illustrates where standard and extended ACLs should be located in an enterprise network.

Say that the objective is to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network. Extended ACLs should be located as close as possible to the source of the traffic to be filtered. This way, undesirable traffic is denied close to the source network, without crossing the network infrastructure.

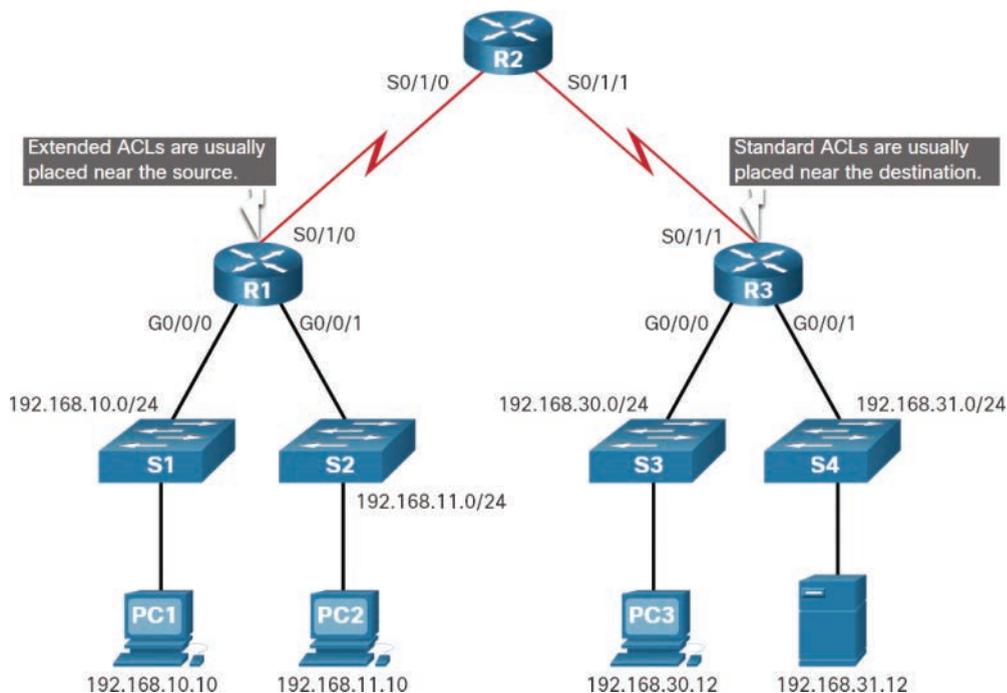


Figure 4-5 Example of Where to Place ACLs

Standard ACLs should be located as close to the destination as possible. If a standard ACL were placed at the source of the traffic, the “permit” or “deny” would occur based on the given source address, regardless of the traffic destination.

Placement of an ACL and, therefore, the type of ACL used, may also depend on a variety of factors, as listed in Table 4-11.

Table 4-11 ACL Placement Factors

Factors Influencing ACL Placement	Explanation
The extent of organizational control	<ul style="list-style-type: none"> Placement of the ACL can depend on whether the organization has control of both the source and destination networks.
Bandwidth of the networks involved	<ul style="list-style-type: none"> It may be desirable to filter unwanted traffic at the source to prevent transmission of bandwidth-consuming traffic.
Ease of configuration	<ul style="list-style-type: none"> It may be easier to implement an ACL at the destination, but traffic will use bandwidth unnecessarily. An extended ACL could be used on each router where the traffic originated. This would save bandwidth by filtering the traffic at the source, but it would require creation of extended ACLs on multiple routers.

Standard ACL Placement Example (4.4.4)

Following the guidelines for ACL placement, standard ACLs should be located as close to the destination as possible.

In Figure 4-6, the administrator wants to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.

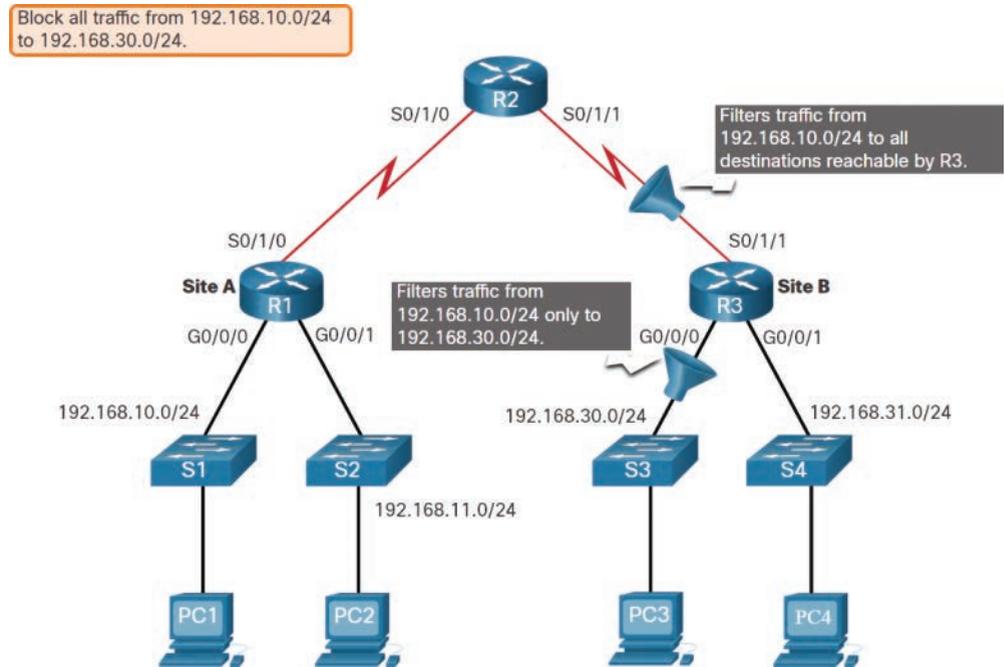


Figure 4-6 Standard ACL Example Topology

Following the basic placement guidelines, the administrator would place a standard ACL on router R3. There are two possible interfaces on R3 to which to apply the standard ACL:

- R3 S0/1/1 interface (inbound):** The standard ACL can be applied inbound on the R3 S0/1/1 interface to deny traffic from the .10 network. However, it would also filter .10 traffic to the 192.168.31.0/24 (.31 in this example) network. Therefore, the standard ACL should not be applied to this interface.
- R3 G0/0 interface (outbound):** The standard ACL can be applied outbound on the R3 G0/0/0 interface. This will not affect other networks that are reachable by R3. Packets from the .10 network will still be able to reach the .31 network. This is the best interface to place the standard ACL to meet the traffic requirements.

Extended ACL Placement Example (4.4.5)

Extended ACLs should be located as close to the source as possible to prevent unwanted traffic from being sent across multiple networks only to be denied when it reaches its destination.

However, an organization can only place ACLs on devices that it controls. Therefore, the extended ACL placement must be determined in the context of where organizational control extends.

In Figure 4-7, for example, Company A wants to deny Telnet and FTP traffic to Company B's 192.168.30.0/24 network from its 192.168.11.0/24 network while permitting all other traffic.

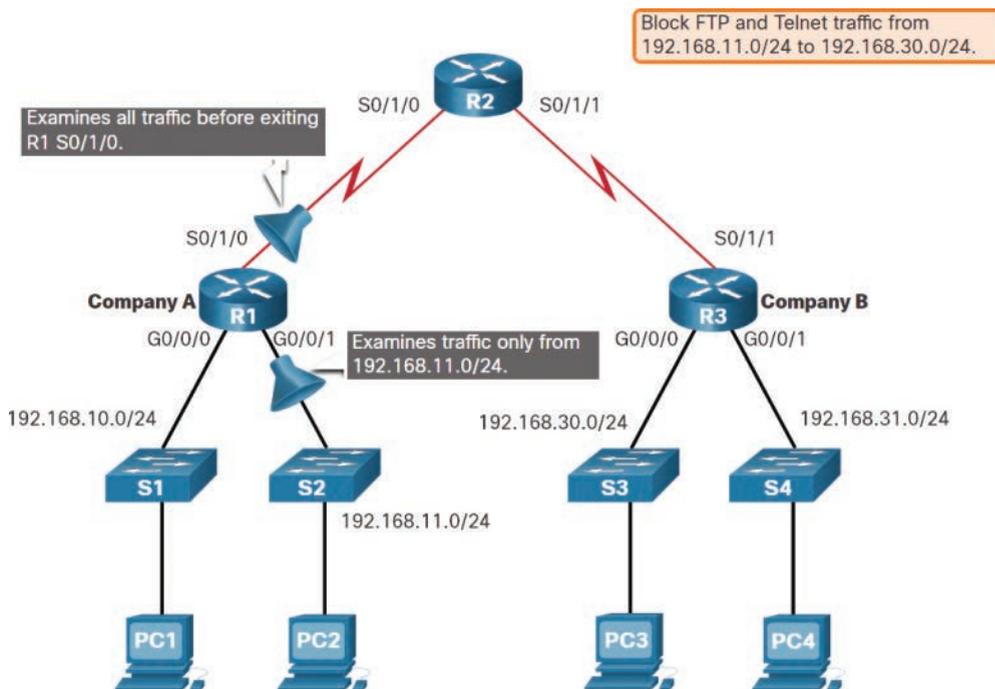


Figure 4-7 Extended ACL Example Topology

There are several ways to accomplish these goals. An extended ACL on R3 would accomplish the task, but the administrator does not control R3. In addition, this solution would allow unwanted traffic to cross the entire network, only to be blocked at the destination, which would affect overall network efficiency.

The solution is to place on R1 an extended ACL that specifies both source and destination addresses. There are two possible interfaces on R1 to apply the extended ACL:

- **R1 S0/1/0 interface (outbound):** The extended ACL can be applied outbound on the S0/1/0 interface. However, this solution would process all packets leaving R1, including packets from 192.168.10.0/24.
- **R1 G0/0/1 interface (inbound):** The extended ACL can be applied inbound on the G0/0/1, and only packets from the 192.168.11.0/24 network are subject to ACL processing on R1. Because the filter is to be limited to only those packets leaving the 192.168.11.0/24 network, applying the extended ACL to G0/1 is the best solution.

**Interactive
Graphic**

Check Your Understanding—Guidelines for ACL Placement (4.4.6)

Refer to the online course to complete this activity.

Summary (4.5)

The following is a summary of the sections in this chapter.

Purpose of ACLs

Several tasks performed by routers require the use of ACLs to identify traffic. An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. A router does not have any ACLs configured by default. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine whether the packets can be forwarded. An ACL uses a sequential list of permit or deny statements, known as ACEs. Cisco routers support two types of ACLs: standard ACLs and extended ACLs. An inbound ACL filters packets before they are routed to the outbound interface. If a packet is permitted by the ACL, it is then processed for routing. An outbound ACL filters packets after being routed, regardless of the inbound interface. When an ACL is applied to an interface, it follows a specific operating procedure:

- Step 1.** The router extracts the source IPv4 address from the packet header.
- Step 2.** The router starts at the top of the ACL and compares the source IPv4 address to each ACE, in sequential order.
- Step 3.** When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
- Step 4.** If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an implicit deny ACE automatically applied to all ACLs.

Wildcard Masks

An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match. Wildcard masks are also used by the Open Shortest Path First (OSPF) routing protocol. A wildcard mask is similar to a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match. However, a wildcard mask and a subnet mask differ in the way they match binary 1s and 0s. Wildcard mask bit 0 matches the corresponding bit value in the address. Wildcard mask bit 1 ignores the corresponding bit value in the address. A wildcard mask is used to filter traffic for one host, one subnet, and a range of IPv4 addresses. A shortcut for calculating a wildcard mask is to subtract the subnet mask from 255.255.255.255. Working with decimal representations of binary wildcard mask bits

can be simplified by using the Cisco IOS keywords **host** and **any** to identify the most common uses of wildcard masking. Keywords reduce ACL keystrokes and make it easier to read ACEs.

Guidelines for ACL Creation

There is a limit on the number of ACLs that can be applied on a router interface. For example, a dual-stacked (that is, IPv4 and IPv6) router interface can have up to four ACLs applied. Specifically, a router interface can have one outbound IPv4 ACL, one inbound IPv4 ACL, one inbound IPv6 ACL, and one outbound IPv6 ACL. ACLs do not have to be configured in both directions. The number of ACLs and the direction in which they are applied to the interface depend on the security policy of the organization. Basic planning is required before configuring an ACL and includes the following best practices:

- Base ACLs on the organization's security policies.
- Write out what you want the ACL to do.
- Use a text editor to create, edit, and save all of your ACLs.
- Document ACLs by using the **remark** command.
- Test the ACLs on a development network before implementing them on a production network.

Types of IPv4 ACLs

There are two types of IPv4 ACLs: standard ACLs and extended ACLs. Standard ACLs permit or deny packets based only on the source IPv4 address. Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more. ACLs 1 to 99 and 1300 to 1999 are standard ACLs. ACLs 100 to 199 and 2000 to 2699 are extended ACLs. Using named ACLs is the preferred method when configuring ACLs. Standard and extended ACLs can be named to provide information about the purpose of each ACL.

The following are basic rules to follow for named ACLs:

- Assign a name to identify the purpose of an ACL.
- Names can contain alphanumeric characters.
- Names cannot contain spaces or punctuation.
- It is suggested that the name be written in CAPITAL LETTERS.
- Entries can be added or deleted within an ACL.

Every ACL should be placed where it has the greatest impact on efficiency. Extended ACLs should be located as close as possible to the source of the traffic to be filtered. This way, undesirable traffic is denied close to the source network without crossing the network infrastructure. Standard ACLs should be located as close to the destination as possible. If a standard ACL were placed at the source of the traffic, the “permit” or “deny” would occur based on the given source address, regardless of the traffic destination. Placement of the ACL may depend on the extent of organizational control, bandwidth of the networks, and ease of configuration.

Practice

The following Packet Tracer activity provides practice with the topics introduced in this chapter. The instructions are available in the companion *Enterprise Networking, Security, and Automation Labs & Study Guide (CCNAv7)* (ISBN 9780136634690). There are no labs for this chapter.

Packet Tracer
Activity

Packet Tracer Activity

Packet Tracer 4.1.4: ACL Demonstration

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix “Answers to the ‘Check Your Understanding’ Questions” lists the answers.

1. What two functions describe uses of access control lists? (Choose two.)
 - A. ACLs assist a router in determining the best path to a destination.
 - B. ACLs can control which areas a host can access on a network.
 - C. ACLs provide a basic level of security for network access.
 - D. Standard ACLs can filter traffic based on source and destination network addresses.
 - E. Standard ACLs can restrict access to specific applications and ports.
2. Which three statements describe how an ACL processes packets? (Choose three.)
 - A. A packet is compared with all ACEs in the ACL before a forwarding decision is made.
 - B. A packet that has been denied by one ACE can be permitted by a subsequent ACE.

- C. An implicit deny at the end of an ACL rejects any packet that does not match an ACE.
 - D. Each ACE is checked only until a match is detected or until the end of the ACL.
 - E. If an ACE is matched, the packet is either rejected or forwarded, as directed by the ACE.
 - F. If an ACE is not matched, the packet is forwarded by default.
3. Which three statements are best practices related to placement of ACLs? (Choose three.)
- A. Filter unwanted traffic before it travels onto a low-bandwidth link.
 - B. For every inbound ACL placed on an interface, ensure that there is a matching outbound ACL.
 - C. Place extended ACLs close to the destination IP address of the traffic.
 - D. Place extended ACLs close to the source IP address of the traffic.
 - E. Place standard ACLs close to the destination IP address of the traffic.
 - F. Place standard ACLs close to the source IP address of the traffic.
4. Which two characteristics are shared by standard and extended ACLs? (Choose two.)
- A. Both filter packets for a specific destination host IP address.
 - B. Both include an implicit deny as a final entry.
 - C. Both permit or deny specific services by port number.
 - D. They both filter based on protocol type.
 - E. They can be created by using either descriptive names or numbers.
5. Which two statement describes a difference between the operation of inbound and outbound ACLs? (Choose two.)
- A. Inbound ACLs are processed before the packets are routed.
 - B. Inbound ACLs can be used in both routers and switches.
 - C. Multiple inbound ACLs can be applied to an interface.
 - D. Multiple outbound ACLs can be applied to an interface.
 - E. Outbound ACLs are processed after the routing is completed.
 - F. Outbound ACLs can be used only on routers.
 - G. Unlike outbound ACLs, inbound ACLs can be used to filter packets with multiple criteria.

6. In which configuration would an outbound ACL placement be preferred over an inbound ACL placement?
 - A. When a router has more than one ACL
 - B. When an interface is filtered by an outbound ACL and the network attached to the interface is the source network being filtered within the ACL
 - C. When an outbound ACL is closer to the source of the traffic flow
 - D. When the ACL is applied to an outbound interface to filter packets coming from multiple inbound interfaces before the packets exit the interface

7. What wildcard mask will match networks 10.16.0.0 through 10.19.0.0?
 - A. 0.252.255.255
 - B. 0.0.255.255
 - C. 0.0.3.255
 - D. 0.3.255.255

8. What type of ACL offers increased flexibility and control over network traffic?
 - A. Extended
 - B. Extensive
 - C. Named standard
 - D. Numbered standard

9. Which statement describes a characteristic of standard IPv4 ACLs?
 - A. They can be configured to filter traffic based on both source IP addresses and source ports.
 - B. They can be created with a number but not with a name.
 - C. They filter traffic based on destination IP addresses only.
 - D. They filter traffic based on source IP addresses only.

10. What wildcard mask will match network 10.10.100.64/26?
 - A. 0.0.0.15
 - B. 0.0.0.31
 - C. 0.0.0.63
 - D. 0.0.0.127

Numbers

3DES (Data Encryption Standard), 152, 338
 3G/4G/5G, 302, 307, 314
 800 series routers, 492
 802.11 (Wi-Fi), QoS traffic marking, 373
 900 series routers, 490
 5500 series routers, 491

A

abstraction layers, virtualization, 589–590
 access
 access attacks, 110–113
 remote access Trojan horses, 107
 access control
 data loss, 98
 troubleshooting, 541
 access layer
 hierarchical network design, 462
 scalable networks, 475
 access points. *See* AP
 accumulating costs, single-area OSPF, 66–67
 ACI (Application Centric Infrastructure), 598, 602
 ANP, 602
 APIC, 602–603
 APIC-EM, 606–608
 Nexus 9000 series switches, 602
 spine-leaf topologies, 603
 ACL (Access Control Lists), 164, 175, 188
 ACE, 164–165
 best practices, 174–175
 creating, 173–175, 183, 188
 defined, 164
 extended ACL, 166, 175–176, 180–181, 203–204,
 220
 editing, 213–214
 named extended IPv4 ACL, 212–216
 numbered extended IPv4 ACL, 204–206,
 209–210
 ports, 207–209

protocols, 206–209
 TCP-established extended ACL, 210–211
 verifying, 216–218
 implicit denies, 167, 182
 inbound ACL filters, 166–167
 limits per interface, 173–174
 log keyword, 542
 modifying, 195–196, 219
 sequence numbers method, 197–198
 text method, 196–197
 named ACL, 177
 modifying, 198–199
 named extended IPv4 ACL, 212–216
 named standard IPv4 ACL, 189–190, 193–195
 NAT pools, 246
 network traffic, 165
 numbered ACL, 176
 numbered extended IPv4 ACL, 204–206,
 209–210
 numbered standard IPv4 ACL, 188–189,
 191–193, 195
 outbound ACL filters, 167
 packet filtering, 164–166
 placement of, 177–181
 purpose of, 164–168, 182
 standard ACL, 166, 175–176, 179, 190, 200–203,
 219–220
 stateful firewall services, 210, 220
 statistics, 199
 tasks using ACL, 165
 traffic flows, 165
 transport layer, troubleshooting, 539–542
 types of, 175–181, 183–184
 verifying, 568–570
 wildcard masks, 168, 182–183
 calculating, 170–172
 examples of, 168–169
 IPv4 address ranges, 170
 IPv4 subnets, 169–170
 keywords, 172–173
 matching hosts, 169–170

addresses

- mapping errors, troubleshooting, 536
- spoofing attacks, 118, 120–121

adjacencies

- BDR, 51, 54–56
- DR, 51, 54–56
- routers, 23–24
- troubleshooting, 539

adjacency databases, OSPF, 5**adware, 108****AES (Advanced Encryption Standard), 152, 338****AF (Assured Forwarding) values, DSCP, 376–377****AH (Authentication Headers), 336****algorithms**

- OSPF, 5
- QoS queuing algorithms, 361, 383
 - CBWFQ, 364
 - FIFO, 362
 - LLQ, 365
 - WFQ, 362–364
- SHA, 146–147, 339
- SPF, 5, 8–9

amplification attacks, 118–120**analyzing**

- cable analyzers, 527
- dynamic NAT, 247–249
- information (troubleshooting process), 514
- PAT, 254–255
- static NAT, 241–242

ANP (Application Network Profiles), 602**Ansible, 643****AnyConnect Secure Mobility Client, 321****AP (Access Points), 288, 485****API (Application Programming Interface), 628–629, 631, 633, 651**

- calls, 630
- example of, 629–630
- internal (private) API, 632
- JSON-RPC, 632–633
- open (public) API, 631–632
- partner API, 632
- REST, 632–639, 651–652
- SOAP, 632
- web service API, 632–633
- XML-RPC, 632–633

APIC (Application Policy Infrastructure Controller), 602–603**APIC-EM (Application Policy Infrastructure Controller-Enterprise Module), 606–608****application layer**

- DNS, 544
- FTP, 544
- HTTP, 544
- NFS, 544
- POP, 544
- SMTP, 544
- SNMP, 544
- SSH, 544
- telnet command, 544
- TFTP, 544
- troubleshooting, 543–545

area ID

- hello packets, 16
- point-to-point OSPF networks, 40

ARP (Address Resolution Protocol)

- cache poisoning, 128–130
- commands, 553–554
- process of, 128
- spoofing attacks, 130
- tables, 553–554, 557
- vulnerabilities, 127–130

arrays, 625**ASA (Adaptive Security Appliances), 140, 321****ASBR (Autonomous System Boundary Routers), 74****ASIC (Application-Specific Integrated Circuits), 485–486****ASR 1000 series routers, 490–491****ASR 9000 series routers, 488–491****assets (security), defined, 96****assigning**

- router ID, 40
- VLAN, troubleshooting, 556–558

asymmetric encryption, 152–156**ATM (Asynchronous Transfer Mode), 296, 324****attacks (security), 109, 158**

- access attacks, 110–113
- address spoofing attacks, 118, 120–121
- amplification attacks, 118–120
- baiting attacks, 114
- buffer overflow attacks, 112–113
- DDoS attacks, 116–117

- DoS attacks, 115–116
 - dumpster diving attacks, 114
 - ICMP attacks, 117–119
 - impersonation attacks, 114
 - IP attacks, 117–122
 - MITM attacks, 112–113, 118
 - password attacks, 111
 - phishing attacks, 114. *See also* spear phishing attacks
 - port redirection attacks, 112
 - pretexting attacks, 114
 - reconnaissance attacks, 109–110
 - reflection attacks, 118–120
 - session hijacking attacks, 118
 - shoulder surfing attacks, 114
 - social engineering attacks, 114–115
 - something for something (quid pro quo) attacks, 114
 - spam attacks, 114
 - spear phishing attacks, 114. *See also* phishing attacks
 - spoofing attacks, 111
 - tailgaiting attacks, 114
 - tools, 101–102
 - trust exploitation attacks, 111
 - types of attacks, 104–105
 - attenuation, troubleshooting, 533**
 - authentication, 339–340**
 - AH, 336
 - HMAC, 147–149, 338–339
 - MD5, 339
 - origin authentication, 144
 - HMAC, 147–149
 - IPsec, 333, 335
 - PSK, 339–340
 - RSA, 340–342
 - SHA, 339
 - authoritative time sources, 401–402, 443–444**
 - automation, 619, 641, 651**
 - API, 628–629, 631, 633, 651
 - calls*, 630
 - example of*, 629–630
 - internal (private) API*, 632
 - JSON-RPC, 632–633
 - open (public) API*, 631–632
 - partner API*, 632
 - REST, 632–639, 651–652
 - SOAP, 632
 - web service API*, 632–633
 - XML-RPC, 632–633
 - benefits of, 619–620
 - Cisco DNA, 647–648
 - Cisco DNA Center, 648–650, 652
 - concept of, 620–621
 - configuration management tools, 639, 642–643, 652
 - Ansible*, 643
 - Chef*, 643
 - CLI*, 639
 - network automation*, 641
 - Puppet*, 643
 - SaltStack*, 643
 - SNMP, 640–641
 - data formats, 620, 628
 - JSON, 622–626
 - key/value pairs*, 622–628
 - rules of*, 622
 - syntax*, 622
 - XML, 623, 627–628
 - YAML, 623, 626–627
 - IBN, 644–646, 652
 - JSON, 622–627
 - arrays*, 625
 - format of*, 623
 - IPv4 addresses*, 625–626
 - JSON-RPC, 632–633
 - syntax*, 624–626
 - smart devices, 620
 - XML, 623, 627–628
 - YAML, 623, 626–627
 - availability, network security, 138**
 - AWA Management Console, 586**
-
- ## B
-
- backbone networks, 287**
 - backhaul networks, 287**
 - backups**
 - configurations from TFTP servers, 428–430, 436
 - IOS images, 437–442
 - baiting attacks, 114**
 - bandwidth, 354**
 - DSL Internet connectivity, 302
 - reference bandwidth, single-area OSPF, 64–66
 - scalable networks, 474–475

baselines, 507–509

baselining tools, 524

performance, troubleshooting, 532, 535

BDR (Backup Designated Routers), 17

adjacencies, 51, 54–56

election

*in OSPF, 20, 23–24**process of, 56–59*

LSA, 24–26

multiaccess OSPF networks, 49–51, 53, 56–59

router priorities, 61–63

BE (Best Effort) values, DSCP, 376**best practices**

ACL, 174–175

network security, 137, 159

*availability, 138**confidentiality, 138**defense-in-depth approach, 138–139**firewalls, 139–140**IDS, 140–141**integrity, 138**IPS, 140–141**layered approach, 138–139***best-effort QoS policy model, 366–367****black hat hackers, 99****blacklisting URL (Uniform Resource Locators), 142****boot sector viruses, 107****boot system, configuring IOS images, 441–442****BOOTP, troubleshooting, 543****borderless switched networks, 458–461****bottlenecks/congestion (networks), troubleshooting, 532****bottom-up troubleshooting method, 518–519****branch networks, 281****branch routers, 488****breaches (security), 95****broadband connectivity**

dedicated broadband WAN connectivity, 297–298

Internet-based broadband WAN connectivity, 298, 314–315

*3G/4G/5G, 302, 307, 314**cable Internet connectivity, 305–306**DSL Internet connectivity, 302–304**ISP Internet connectivity, 309–310**LTE, 307**solution comparisons, 311**teleworking, 283, 302, 308, 312, 314**wired Internet connectivity, 301–302**wireless Internet connectivity, 302**wireless Internet-based broadband connectivity, 306–307***broadcast multiaccess networks, 49, 84****broadcasts, troubleshooting, 536****buffer overflow attacks, 112–113****buffered logging, 529****building switch blocks, 474****business considerations for switch selection, 486–487**

C**cable analyzers, 527****cable modems, 288****cable testers, 526–527****cabling**

DOCSIS, 305

faults, troubleshooting, 533

fiber optic Internet connectivity, 305–306

HFC networks, cable modems, 305

Internet connectivity, 305

optical nodes, 305

SDH cabling standard, 291–292

SONET cabling standard, 291–292

calendar services, network management, 400**CAM tables, spoofing attacks, 121****campus LAN switches, 477–478****campus networks, 280****carrier protocols, 329****carrier WAN connections, 278**

dual-carrier WAN connections, 278–279

single-carrier WAN connections, 278

Catalyst 2960-C series switches, 485–486**Catalyst 3560-C series switches, 485****causes of network problems, troubleshooting, 573–574**

data link layer, 534–537

physical layer, 531–534

CBWFQ (Class-Based Weight Fair Queuing), 364**CDP (Cisco Discovery Protocol), 390–396, 441–442****CEF (Cisco Express Forwarding), Layer 3 switches, 596****cellular Internet connectivity, 306–307**

- central controller and SDN, 597
- changing passwords, 435
- Chef, 643
- circuit-switched network communications, 290
- circuit-switched WAN connectivity, 295
- Cisco DNA Assurance, 648
- Cisco DNA Center, 648–650, 652
- Cisco DNA (Digital Network Architecture), 647–648
- Cisco DNA Security, 648
- classification/marketing tools (QoS), 371–372
- classifying traffic, 362–363, 368
- CLI (Command Line Interface), 639
- client-based VPN, 321, 326
- clientless VPN, 326
- clock (software)
 - setting manually, 400
 - source, displaying, 403
- cloud computing, 583, 585–586, 609
 - cloud services, 584
 - cloud-managed switches, 478
 - community clouds, 585
 - data centers versus, 585
 - hybrid clouds, 584–585
 - IaaS, 584
 - PaaS, 584
 - private clouds, 584
 - public clouds, 584
 - SaaS, 584
 - storage devices, data loss, 98
- CnC (Command and Control), 116–117, 132–133
- CO (Central Office), WAN, 286
- code delays, 355
- collapsed core network design, 464
- collecting data, IOS commands, 511–512
- communications (network)
 - circuit-switched network communications, 290
 - demodulation, 288, 295
 - DWDM multiplexing, 292
 - jitter, 291, 294, 355
 - latency, 291, 294, 302, 314
 - modulation, 288, 295
 - packet-switched network communications, 290–291
 - ATM, 296, 324
 - Frame Relay networks, 295–296
 - parallel network communications, 289
 - SDH cabling standard, 291–292
 - serial network communications, 289
 - SONET cabling standard, 291–292
- community clouds, 585
- community strings (SNMP), 412–415
- comparison troubleshooting method, 522
- compromised-key attacks, 105
- confidentiality
 - data confidentiality, 144, 150
 - IPsec, 333–334, 336–338
 - network security, 138
- configuration register, password recovery, 433–435, 437
- configuring
 - CDP, 391–393
 - configuration management tools, 639, 642–643, 652
 - Ansible, 643
 - Chef, 643
 - CLI, 639
 - network automation, 641
 - Puppet, 643
 - SaltStack, 643
 - SNMP, 640–641
 - dynamic NAT, 245–247, 251
 - LLDP, 397
 - NAT, 260
 - networks
 - CLI, 639
 - SNMP, 640–641
 - NTP, 402–405
 - OSPF
 - ipospf command, 43–44
 - network command, 41–43
 - router priorities, 61–63
 - PAT
 - address pools, 253
 - single IP addresses, 252
 - point-to-point OSPF networks, 49
 - restoring configurations from, text files, 428–430
 - routers
 - copying configurations, 431
 - ID, 38–39
 - restoring configurations, 432
 - saving configurations, 435
 - verifying configurations, 432
 - static NAT, 240–241

- switches
 - fixed configuration switches*, 480
 - modular configuration switches*, 480
 - stackable configuration switches*, 481
- Syslog, 422–423
- Syslog traps, 530–531
- congestion**, 353–354
 - avoidance tools, 371, 379–380
 - management tools, 371, 379–380
 - troubleshooting, 532
- connectivity**
 - IP connectivity, troubleshooting, end-to-end connectivity, 545–549
 - loss of, 532
 - troubleshooting, 535, 539
 - WAN connectivity
 - 3G/4G/5G, 302, 307, 314
 - cable Internet connectivity*, 305–306
 - circuit-switched WAN connectivity*, 295
 - dedicated broadband WAN connectivity*, 297–298
 - DSL Internet connectivity*, 302–304
 - Internet-based broadband WAN connectivity*, 298, 301–311, 314–315
 - ISDN, 295
 - ISP Internet connectivity*, 309–310
 - leased-line WAN connectivity*, 293–294
 - LTE, 307
 - Metro Ethernet WAN connectivity*, 298–300, 332
 - modern WAN connectivity*, 296–301, 314
 - MPLS, 298, 300–301, 324, 332
 - packet-switched WAN connectivity*, 298
 - PSTN, 295
 - solution comparisons*, 311
 - teleworking*, 283, 302, 308, 312, 314
 - traditional WAN connectivity*, 292–296, 312–313
 - wired Internet connectivity*, 301–302
 - wireless Internet connectivity*, 302
 - wireless Internet-based broadband connectivity*, 306–307
 - wireless connectivity, scalable networks, 466–467
- console error messages**, troubleshooting, 533
- console logging**, 529
- console messages**, troubleshooting, 536
- content security appliances**
 - ESA, 142
 - WSA, 142–143
- control plane**, SDN, 595
- controller-based SDN**, 605, 611–612
- converged networks**, 458, 493
- convergence**
 - link-state operation, 6
 - OSPF routers, 17–26
- converters (optical)**, 288
- copying**
 - IOS images to TFTP servers, 439–440
 - router configurations to USB drives, 431–432
- core devices (WAN)**, 288
- core layer (hierarchical network design)**, 462
- CoS traffic marking**, 373–374, 377–378
- cost metrics**
 - single-area OSPF, 63–64
 - accumulating costs*, 66–67
 - manually setting cost value*, 66–67
 - reference bandwidths*, 65
 - switches, 486
 - VPN, 322
- CPE (Customer Premises Equipment)**, 286
- CPU (Central Processing Units)**
 - high utilization rates, troubleshooting, 533
 - overloads, troubleshooting, 534
- cryptography**, 143, 156, 159
 - data confidentiality, 144, 150
 - data integrity, 144–145
 - data nonrepudiation, 144
 - encryption
 - 3DES, 152
 - AES, 152
 - asymmetric encryption*, 152–156
 - DES, 152
 - DH, 154–156
 - DSA, 154
 - DSS, 154
 - ElGamal, 154
 - elliptic curve cryptography*, 154
 - public key algorithms*, 152–156
 - RC series algorithms*, 152
 - RSA, 154
 - SEAL, 152
 - symmetric encryption*, 151–152
 - hash functions, 144
 - MD5, 145
 - SHA, 146–147
 - origin authentication, 144, 147–149

CS (Class Selector) bits, DSCP, 377–378
 CSU (Channel Service Units), 288
 cybercriminals, 100
 cybersecurity (current state of), 95, 157. *See also*
 security
 assets, 96
 breaches, 95
 current state of affairs, 95–96
 cybercriminals, 95
 exploits, 96
 mitigation, 96
 risk, 96
 threats, 96
 vectors of
 data loss, 97–98
 network attacks, 96–97
 vulnerabilities, 96

D

dark fiber, 297–298
 data centers
 cloud computing versus, 585
 switches, 478
 data collection, IOS commands, 511–512
 data confidentiality, 144, 150
 data delays, 360–361
 data exfiltration, 97–98
 data formats, 620, 628
 concept of, 620–621
 JSON, 622–624, 626–627
 arrays, 625
 IPv4 addresses, 625–626
 JSON-RPC, 632–633
 syntax, 624–626
 key/value pairs, 622–628
 rules of, 622
 syntax, 622, 624–626
 XML, 623, 627–628
 YAML, 623
 data integrity, 144–145, 333, 335, 338–339
 data link layer (networks), troubleshooting, 534–537
 data loss vectors (security), 97–98
 data measurement, network documentation,
 510–512
 data modification attacks, 105
 data nonrepudiation, 144
 data plane, SDN, 596
 data sending Trojan horses, 107
 data structures, OSPF, 4–5
 data traffic, 357, 360–361
 databases
 adjacency databases, 5
 forwarding databases, 5
 LSDB 5, 7
 OSPF, 5, 20–22
 topology databases, troubleshooting, 539
 DBD (Database Description) packets, 13–14, 21–22
 DCE (Data Communications Equipment), 286–288
 DDoS (Distributed Denial of Service) attacks,
 116–117
 dead intervals, 16, 70–73
 debug command, 517
 debuggers, 104
 dedicated broadband WAN connectivity, 297–298
 dedicated servers, virtualization, 586–587
 default gateways, verifying, 558–560
 IPv4, 559
 IPv6, 560–562
 defense-in-depth approach (network security),
 138–139
 defining problems (troubleshooting process), 514
 de-jitter delays, 355
 delays, 353
 code delays, 355
 data delays, 360–361
 de-jitter delays, 355
 fixed delays, 355
 jitter, 291, 294, 355
 packetization delays, 355
 payout delay buffers, 355–356
 propagation delays, 355
 queuing delays, 355
 serialization delays, 355
 variable delays, 355
 demarcation points, 286
 demodulation, 288, 295
 Denial of Service. *See* DoS attacks
 density (port), switches, 482, 486
 departmental switch blocks, 474
 DES (Data Encryption Standard), 152, 338
 design limits, troubleshooting, 534

designing networks, 455

borderless switched networks, 458–461

collapsed core network design, 464

hierarchical networks, 493

*access layer, 462, 475**borderless switched networks, 458–461**core layer, 462**distribution layer, 462*

OSPF, 476–477

*scalability, 455–458**switched networks, 464–465**three-tier network design, 455, 460, 463**two-tier network design, 461, 464*

line cards, 480, 482

routers, 494–495

*800 series routers, 492**900 series routers, 490**5500 series routers, 491**ASR 1000 series routers, 490–491**ASR 9000 series routers, 490–491**branch routers, 488**fixed configuration routers, 492**form factors, 490–492**industrial routers, 490, 492**modular routers, 492**network edge routers, 488–489**requirements, 487–488**service provider routers, 489*

scalable networks, 465–466, 477, 493–494

*access layer, 475**bandwidth, 474–475**failure domains, 469–474**hierarchical networks, 455–458**multiple links, 466–467**redundancy plans, 469**redundant links, 466–467**scalable routing protocol, 467–468**tuning routing protocols, 476–477**wireless connectivity, 465–466*

SFP devices, 482

switches, 477, 487, 494–495

*ASIC, 485–486**business considerations for switch selection, 486–487**campus LAN switches, 477–478**Catalyst 2960-C series switches, 485–486**Catalyst 3560-C series switches, 485**cloud-managed switches, 478**data center switches, 478**fixed configuration switches, 480**form factors, 479–481**forwarding rates, 483**modular configuration switches, 480**multilayer switching, 485–486**platforms, 477–479**PoE, 484–486**port density, 482**RU, 481, 494**service provider switches, 479**stackable configuration switches, 481**thickness of switches, 481**virtual networks, 479**wire speeds, 483*

three-tier network design, 455, 460, 463

two-tier network design, 461, 464

virtual networks, switches, 479

destination ports, troubleshooting, 541**destructive Trojan horses, 107****device discovery**

CDP, 390–396, 443

LLDP, 396–400, 443

device documentation (networks), 505, 512

end-system documentation files, 506–507

routers, 505–506

switches, 506

device-based SDN, 604–605**DH (Diffie-Hellman), 154–156****DHCP (Dynamic Host Configuration Protocol), 133**

rogue DHCP servers, 121, 134–136

spoofing attacks, 134–136

troubleshooting, 543

dialup modems. See voiceband modems**Diffie-Hellman key exchanges, 333, 335, 342–343****DiffServ (Differentiated Services), 366, 369–370****digital certificates, 327, 333, 335, 339, 341–342, 344–345****digital multimeters (DMM), 525–526****Dijkstra's algorithm, 5****disaster recovery, virtualization, 589****discovering devices**

CDP, 390–396, 443

LLDP, 396–400, 443

- distributed networks, 282
 - distribution layer (hierarchical network design), 461–462, 493
 - divide-and-conquer troubleshooting method, 520–521
 - DLCI (Data-Link Connection Identifiers), 296
 - DMM (Digital Multimeters), 525–526
 - DMVPN (Dynamic Multipoint VPN), 330–331
 - DNS (Domain Name System), 131, 544
 - domain shadowing attacks, 132
 - open resolver attacks, 131
 - stealth attacks, 132
 - traffic analysis, 136
 - troubleshooting, 543
 - tunneling, 132–133
 - verifying, 570–571
 - DOCSIS (Data Over Cable Service Interface Specification), 305
 - documentation, networks, 502, 572
 - baselines, 507–509
 - device documentation, 505, 512
 - data measurement*, 510–512
 - end-system documentation files*, 506–507
 - routers*, 505–506
 - switches*, 506
 - logical network topologies, 504–505
 - overview of, 502
 - physical network topologies, 503
 - domain shadowing attacks, 132
 - DoS (Denial of Service) attacks, 105, 107, 115–116
 - Down state, 17–19
 - DR (Designated Routers), 16
 - adjacencies, 51, 54–56
 - election
 - in OSPF*, 20, 23–24
 - process of*, 56–59
 - failures/recovery, 58–59
 - LSA, 24–26
 - multiaccess OSPF networks, 49–51, 53–54, 56–59
 - router priorities, 61–63
 - single-area OSPF, router ID, 36
 - drives (USB)
 - copying router configurations to, 431–432
 - displaying contents of, 430
 - verifying connections, 430–431
 - DROTHER, 25, 50–51, 52–53
 - DSA (Digital Signature Algorithm), 154
 - DSCP (Differentiated Services Code Points), 375–378
 - DSL (Digital Subscriber Line) Internet connectivity, 302–303
 - bandwidth space allocation, 302
 - DSLAM, 303
 - example of, 303
 - modems, 288
 - PPP, 303–304
 - DSP (Digital Signal Processors), 357
 - DSS (Digital Signature Standard), 154
 - DSU (Data Service Units), 288
 - DTE (Data Terminal Equipment), 286–288
 - dual stacks, 259, 263
 - dual-carrier WAN connections, 278–279
 - dual-homed ISP connectivity, 309
 - dual-homed WAN topology, 276
 - dual-multihomed ISP connectivity, 310
 - dumpster diving attacks, 114
 - duplex mismatches, troubleshooting, 551–553
 - DWDM multiplexing, 292
 - dynamic NAT (Network Address Translation), 232–233, 244–245, 260–261
 - analyzing, 247–249
 - configuring, 245–247, 251
 - topologies, 244–245
 - verifying, 249–251
- ## E
-
- eavesdropping attacks, 105
 - E-carriers, 294
 - edge routers, 74
 - failure domains, 470–471
 - network edge routers, 488–489
 - educated guess troubleshooting method, 522
 - EF (Expedited Forwarding) values, DSCP, 376
 - egress packets, 372
 - ElGamal, 154
 - eliminating probable cause (troubleshooting process), 514
 - elliptic curve cryptography, 154
 - email
 - data loss, 98
 - POP, 544
 - SMTP, 544

EMI (Electromagnetic Interference), troubleshooting,
534

encapsulating

errors, troubleshooting, 536

protocols (IPsec), 336

encryption

3DES, 338

AES, 152, 338

asymmetric encryption, 152–156

DES, 152, 338

DH, 154–156

DSA, 154

DSS, 154

ElGamal, 154

elliptic curve cryptography, 154

encryption protocols, troubleshooting, 542

protocols, troubleshooting, 543

public key algorithms, 152–156

RC series algorithms, 152

RSA, 154

SEAL, 152, 338

symmetric encryption, 151–152

tools, 104

end users (troubleshooting process), questioning,

515–516

endpoint groups (EPG), 602

end-system documentation files, 506–507

end-to-end IP connectivity, troubleshooting

components of, 545–547

IPv4

pinging, 547–548

traceroute command, 548

IPv6

pinging, 548–549

traceroute command, 548–549

reference topologies, 545–547

enterprise networks, 458, 477, 487, 491, 493–494

enterprise VPN (Virtual-Private Networks),

324–325

EoMPLS. See Metro Ethernet WAN connectivity

EPG (Endpoint Groups), 602

error messages (console), troubleshooting, 533

ESA (Email Security Appliance), 142

ESP (Encapsulation Security Protocol), 336

established keyword, troubleshooting, 542

Ethernet

CoS traffic marking, 373–374, 377–378

Metro Ethernet WAN connectivity, 298–300, 332

network adjacencies, 23–24

PoE, switches, 484–486

PPPoE, DSL Internet connectivity, 303–304

QoS traffic marking, 373

WAN, 297–298

ethical hacking, 95

excessive broadcasts, troubleshooting, 536

Exchange state, 18

exfiltration of data, 97–98

exploits (security), defined, 96

ExStart state, 18

extended ACL (Access Control Lists), 166, 175–176,

180–181, 203–204, 220

editing, 213–214

named extended IPv4 ACL, 212–216

numbered extended IPv4 ACL, 204–206, 209–210

ports, 207–209

protocols, 206–209

TCP-established extended ACL, 210–211

verifying, 216–218

F

failover tests to backup routes, single-area OSPF, 69

failure domains

edge routers, 470–471

scalable networks, 469–474

failures/recovery

routers, multiaccess OSPF networks, 58–59

single point of failure, 275, 278

FIB (Forwarding Information Base), 596

fiber optic Internet connectivity, 305–306

FIFO (First-In, First-Out), 362

file systems

Flash file systems, 425

IOS File System, 424, 437–442

NVRAM file systems, 425–426

restoring configurations from, text files, 428–430

router file systems, 423–425, 445–446

switch file systems, 426–427, 445–446

filtering

network traffic with ACL

inbound ACL filters, 166–167

outbound ACL filters, 167
 URL, 142
 firewalls, 139–140, 210, 220
 firmware viruses, 107
 fixed configuration routers, 492
 fixed configuration switches, 480
 fixed delays, 355
 Flash
 backing up configurations from, 436
 file systems, 425
 IOS images, verifying size of, 439–441
 flexibility, borderless switched networks, 459
 flood attacks
 TCP SYN flood attacks, 124
 UDP flood attacks, 127
 flooding LSA, 23–24
 flow control, TCP, 123
 flow tables (switches), 601
 flowcharts (troubleshooting), 512–513
 follow-the-path troubleshooting method, 521–522
 forensic tools, 103
 form factors
 routers, 490–492
 SFP devices, 482
 switches, 479–481
 forwarding databases, OSPF, 5
 Forwarding Information Base (FIB), 596
 forwarding rates (switches), 483
 frame buffers, switches, 487
 Frame Relay networks, 295–296
 framing errors, troubleshooting, 537
 FTP (File Transfer Protocol), 107, 544
 FTTB (Fiber-to-the-Building) Internet connectivity, 306
 FTTH (Fiber-to-the-Home) Internet connectivity, 306
 FTTN (Fiber-to-the-Node/Neighborhood) Internet connectivity, 306
 FTTx Internet connectivity, 305–306
 Full state, 18
 full-duplex, 551–553
 fully meshed WAN topology, 276
 functionality, troubleshooting, 535
 fuzzers, 103

G

gateways (default), verifying, 558–560
 IPv4, 559
 IPv6, 560–562
 gathering information (troubleshooting process), 514, 516–517
 general network issues, troubleshooting, 539
 general troubleshooting procedures, 512–513
 get operations (SNMP), 406–407
 global NAT addresses, 229–231
 gray hat hackers, 99
 GRE (Generic Routing Encapsulation)
 GRE over IPsec, 328–329
 mGRE, 330–331
 group tables (switches), 602

H

hackers, 98–100
 hacking
 OS, 104
 tools, 103
 hacktivists, 100
 half-duplex, 551–553, 575
 hard copies, data loss, 98
 hardware, troubleshooting
 faults, 533
 tools
 cable analyzers, 527
 cable testers, 526–527
 DMM, 525–526
 portable network analyzers, 528
 Prime NAM, 528
 Syslog server, 529–531
 hash functions
 MD5, 145
 SHA, 146–147
 headend, 305
 headers
 TCP headers, 122
 UDP headers, 126
 hello intervals, 16
 hello packets, 13–17
 intervals, single-area OSPF, 69–73
 neighbor adjacencies, OSPF link-state operation, 6

HFC networks, cable modems, 305

hierarchical networks, 493

access layer, 462, 475

borderless switched networks, 458–461

core layer, 462

designing, OSPF, 476–477

distribution layer, 461–462, 493

OSPF, 476–477

scalability, 455–458

switched networks, 464–465

three-tier network design, 455, 460, 463

two-tier network design, 461, 464

hierarchical topologies, multi-area OSPF, 11

high CPU utilization rates, troubleshooting, 533

HMAC (Hash Message Authentication Code), 147–149, 338–339

HTTP (Hypertext Transfer Protocol), 544, 634–639

hub routers, 275–276

hub-and-spoke WAN topology, 275, 330–331

hybrid clouds, 584–585

hypervisors, 588, 591–593

hypotheses (troubleshooting process)

proposals, 514

testing, 515

IaaS (Infrastructure as a Service), 584

IBN (Intent-Based Networking), 644–646, 652

ICMP attacks, 117–119

ID

area ID, point-to-point OSPF networks, 40

router ID, 16, 40, 83

assigning, 40

choosing, 36–37

configuration mode, 35

configuring, 38–39

DR election, 36

loopback interfaces, 37–38

modifying, 39–40

order of precedence, 36–37

reference topologies, 34–35, 38

rid values, 37

synchronization of OSPF databases, 36

verifying, 38–39

IDS (Intrusion Detection Systems), network security, 140–141

IEEE 802.1p. *See* CoS traffic marking

IFS (IOS File System), 424, 437–442

IKE (Internet Key Exchange), 335

images (IOS), managing, 446

backups, 438–441

boot system configurations, 441–442

TFTP backups, 437–442

impersonation attacks, 114

implicit denies, 167, 182, 541

inbound ACL filters, 166–167

industrial routers, 490, 492

information (troubleshooting process)

analyzing, 514

gathering, 514, 516–517

ingress packets, 372

Init state, 17–19

input errors, troubleshooting, 551

input queue drops, 550

inside NAT addresses, 229–231

integrity

of data, 144–145, 333, 335, 338–339

network security, 138

interfaces, *show interfaces* command, 549–550

interference, troubleshooting, 534

internal (private) API, 632

Internet-based broadband WAN connectivity, 298, 314–315

3G/4G/5G, 302, 307, 314

cable Internet connectivity, 305–306

DSL Internet connectivity, 302, 303

bandwidth space allocation, 302

DSLAM, 303

example of, 303

PPP, 303–304

ISP Internet connectivity

dual-homed ISP connectivity, 309

dual-multihomed ISP connectivity, 310

multihomed ISP connectivity, 309–310

single-homed ISP connectivity, 309

LTE, 307

microwave Internet connectivity. *See* WiMAX

solution comparisons, 311

teleworking, 283, 302, 308, 312, 314

wired Internet connectivity, 301–302

- wireless Internet connectivity, 302
- wireless Internet-based broadband connectivity, 306, 308
 - cellular Internet connectivity, 306–307*
 - municipal Wi-Fi Internet connectivity, 306*
 - satellite Internet connectivity, 307*
 - WiMAX, 307*
- interoperability areas (transport layer), troubleshooting, 542–543**
- IntServ (Integrated Services), 366–368**
- IOS commands**
 - data collection, 511–512
 - gathering information (troubleshooting process), 516–517
- IOS File System, 424, 437–442, 446**
- IOS log messages, severity levels (Syslog), 530**
- IP (Internet Protocol)**
 - show ip interface brief command, 517
 - show ip route command, 517
- IP addresses, attacks, 105, 117–122, 158. *See also* security**
- IP connectivity, troubleshooting, 574–576**
 - ACL, verifying, 568–570
 - DNS, verifying, 570–571
 - end-to-end connectivity
 - components of, 545–547*
 - duplex mismatches, 551–553*
 - IPv4 ping, 547–548*
 - IPv4 traceroute command, 548*
 - IPv6 ping, 548–549*
 - IPv6 traceroute command, 548–549*
 - reference topologies, 545–547*
 - verifying physical layer, 549–551*
 - local network addressing, end-to-end connectivity, 553–556
 - network paths, verifying, 562–566
 - transport layer, verifying, 566–567
 - verifying physical layer, 549–551
 - VLAN assignments, 556–562
- IP phone, PoE, 484**
- IP services, 127–130, 158**
- ipospf command, point-to-point OSPF networks, configuring OSPF, 43–44**
- ipospf priority command, 61**
- IPP (IP Precedence), 373, 375, 377–378**
- IPS (Intrusion Prevention Systems), 140–141**
- IPsec (IP Security), 332–345. *See also* VPN**
 - AH, 336
 - authentication, 339–340
 - PSK, 339, 340*
 - RSA, 340–342*
 - confidentiality, 333–334, 336–338
 - data integrity, 333, 335, 338–339
 - Diffie-Hellman key exchanges, 333, 335, 342–343
 - ESP, 336
 - framework of, 334–335
 - GRE over IPsec, 328–329
 - origin authentication, 333, 335
 - protocol encapsulation, 336
 - SA, 334–335
 - SSL comparisons, 326–327
 - transport and tunnel mode, 343
 - VTI, 331–332
- IPv4 (Internet Protocol version 4)**
 - ACL, 175, 188. *See also* extended ACL; named ACL; numbered ACL; standard ACL
 - creating, 188*
 - modifying, 195–198, 219*
 - placement of, 177–181*
 - stateful firewall services, 210, 220*
 - statistics, 199*
 - wildcard masks, 168–173*
 - addressing
 - ranges, wildcard masks, 170*
 - troubleshooting, 541*
 - ARP tables, 553–554
 - attacks, 117–118
 - default gateways, 559
 - extended ACL, 175–176, 180–181, 203–204, 220
 - editing, 213–214*
 - named extended IPv4 ACL, 212–216*
 - numbered extended IPv4 ACL, 204–206, 209–210*
 - ports, 207–209*
 - protocols, 206–209*
 - TCP-established extended ACL, 210–211*
 - verifying, 216–218*
 - JSON, 625–626
 - logical network topologies, 504
 - named ACL, 177
 - modifying, 198–199*
 - named extended IPv4 ACL, 212–216*
 - named standard IPv4 ACL, 189–190, 193–195*

NAT, 226, 237

- advantages of*, 238, 261
- configuring*, 260
- defined*, 227–228
- disadvantages of*, 238–239, 261
- dynamic NAT*, 232–233, 244–251, 260–261
- global NAT addresses*, 229–231
- inside global NAT addresses*, 230
- inside local NAT addresses*, 230–231
- inside NAT addresses*, 227–231
- local NAT addresses*, 229–231
- NAT overload*. *See* PAT
- NAT64*, 258–259
- NAT-PT*, 259
- operation of*, 228–229
- outside global NAT addresses*, 231
- outside local NAT addresses*, 231
- outside NAT addresses*, 229, 231
- PAT*, 233–234, 237, 251–257, 260–261
- pools*, 245–247
- private IPv4 addresses*, 226–227
- static NAT*, 231–232, 239–244, 260–261
- stub networks*, 228
- terminology*, 229–231
- troubleshooting*, 542–543

numbered ACL, 176

- numbered extended IPv4 ACL*, 204–206, 209–210
- numbered standard IPv4 ACL*, 188–189, 191–193, 195

packet headers, 374–375

pinging, 547–548

private addresses, 226–227

QoS traffic marking, 373

standard ACL, 175–176, 179, 190, 200–203, 219–220

subnets, wildcard masks, 169–170

traceroute command, 548

Type of Service field, 375

wildcard masks

- address ranges*, 170
- subnets*, 169–170
- troubleshooting*, 541

IPv6 (Internet Protocol version 6)

- attacks, 117–118
- default gateways, 560–562

- logical network topologies, 505
- NAT64, 258–259
- neighbor tables, 554–555
- packet headers, 374–375
- pinging, 548–549
- QoS traffic marking, 373
- show ipv6 interface brief command, 517
- show ipv6 route command, 517
- traceroute command, 548–549
- Traffic Class field, 375

ISDN (Integrated Services Digital Networks), 295

ISP (Internet Service Providers)

- Internet connectivity
 - dual-homed ISP connectivity*, 309
 - dual-multihomed ISP connectivity*, 310
 - MPLS VPN*, 332
 - multihomed ISP connectivity*, 309–310
 - single-homed ISP connectivity*, 309
 - VPN*, 324–325
- routers, 489
- switches, 479
- VPN, 324–325

ISR 4000 series routers, 488

J

- jabber, 533
- jitter, 291, 294, 355
- JSON (JavaScript Object Notation)**, 622–624, 626–627
 - arrays, 625
 - format of, 623
 - IPv4 addresses, 625–626
 - JSON-RPC, 632–633
 - syntax, 624–626
- JSON-RPC (JavaScript Object Notation-Remote Procedure Call)**, 632–633

K

- keylogger attacks, 107
- keys (security), compromised-key attacks, 105
- key/value pairs, 622–628
- knowledge bases, 524

L

LAN (Local-Area Networks)
 campus LAN switches, 477–478
 switches, device documentation, 506
 WAN comparisons, 272–273

last mile (local loops), 286

latency, 291, 294, 302, 314

Layer 2 MPLS VPN, 324, 332, 344

Layer 2 QoS traffic marking, 373–374

Layer 2 traffic marking, 373–374

Layer 3 MPLS VPN, 324, 332, 334, 344

Layer 3 switches, SDN, 596

Layer 3 traffic marking, 374–375

layered approach (network security), 138–139

layered models, troubleshooting with, 517–518

leased-line WAN connectivity, 293–294

legacy support, virtualization, 589

line cards, 480, 482

links, scalable networks
 multiple links, 466–467
 redundant links, 466–467

link-state operation
 convergence, 6
 OSPF, 6
establishing neighbor adjacencies, 6
LSA, 6–7
LSDB, 7
SPF algorithms, 8–9
SPF trees, 8–9
 route selection, 8–9

link-state routing protocols. *See* OSPF

list of neighbors, 17

LLDP (Link Layer Discovery Protocol), 396–400, 443

LLQ (Low Latency Queuing), 365

Loading state, 18

local loops (last mile), 286

local NAT addresses, 229–231

local network addressing, verifying, 553–556

log keyword, ACL, 542

logging
 buffered logging, 529
 console logging, 529
 logging trap command, 530

logical network topologies, 504–505

loopback interfaces

point-to-point OSPF networks, 48
 router ID, 37–38

loops

local loops (last mile), 286
 STP loops, troubleshooting, 537

LSA (Link-State Advertisements)

BDR, 24–26
 DR, 24–26
 exchanging, OSPF, 6–7
 flooding, 23–24
 LSU packets, 14

LSAck (Link-State Acknowledgement) packets, 13–14

LSDB (Link-State Databases)

OSPF, 5, 7
 topology tables, 7

LSR (Label-Switched Routers), 300–301

LSR (Link-State Request) packets, 13–14, 22

LSU (Link-State Update) packets, 13–14

LTE (Long-Term Evolution), 307

M

MAC addresses

spoofing attacks, 120–121
 switch MAC address tables, 555–557

macros, viruses, 107

malware, 106, 108–109, 157

adware, 108
 overview of, 106
 ransomware, 108
 rootkits, 108
 spyware, 108
 Trojan horses, 106–107
 viruses, 106–107
 worms, 106, 108

management plane, SDN, 598

managing networks, 390

calendar services, 400
 CDP, 390–396, 443
 configurations
backups, 428–430, 436
restoring from text files, 428–430
 IOS images, 424, 437–442
 LLDP, 396–400, 443

NTP, 400–405, 443–444
passwords
 changing, 435
 recovery, 433–437
routers
 copying configurations, 431
 file systems, 423–424, 445–446
 restoring configurations, 432
 saving configurations, 435
 USB ports, 430
 verifying configurations, 432
SNMP, 405–418, 444
switch file systems, 426–427, 445–446
Syslog, 418–423, 444–445
time services, 400
USB drives
 copying router configurations to, 431–432
 displaying contents of, 430
 verifying connections, 430–431
man-in-the-middle attacks. *See* MITM
marking/classification tools (QoS), 371–372
MD5 (Message-Digest 5), 339
MD5 hash function, 145
measuring data, network documentation, 510–512
meter tables (switches), 602
Metro Ethernet WAN connectivity, 298–300, 332
mGRE (Multipoint GRE), 330–331
MIB (Management Information Base)
 OID, 415
 variables, SNMP agents, 407
microwave Internet connectivity. *See* WiMAX
mission-critical services, 455–456, 490
mitigation (security), defined, 96
MITM (Man-in-the-Middle) attacks, 105, 112–113, 118
modems
 cable Internet connectivity, 305
 cable modems, 288
 CSU, 288
 dialup modems. *See* voiceband modems
 DSL modems, 288
 DSU, 288
 voiceband modems, 288
modern WAN connectivity, 296–301, 314
modifying
 ACL, 195–196, 219

named ACL, 198–199
 sequence numbers method, 197–198
 text method, 196–197
 router ID, 39–40
 single-area OSPF, 85–86
modular configuration switches, 480
modular routers, 492
modularity, borderless switched networks, 459
modulation, 288, 295
MPLS (Multi-Protocol Label Switching), 298, 300–301, 324
 Layer 2 MPLS VPN, 324, 332, 344
 Layer 3 MPLS VPN, 324, 332, 334, 344
 QoS traffic marking, 373
 VPN, 332
multiaccess OSPF networks, 49
 adjacencies, 54–56
 designated routers, 49–51
 election process, 56–59
 reference topologies, 51–52, 57
 router election process, 56–59
 router failures/recovery, 58–59
 router priorities, 61–63
 verifying router roles, 52–54
multi-area OSPF, 9–11
multihomed ISP connectivity, 309–310
multilayer switching, 485–486
multimeters (digital), 525–526
multiple adjacencies, routers, 23–24
multiple links, scalable networks, 466–467
municipal Wi-Fi Internet connectivity, 306

N

NAM (Network Analysis Module), 528
named ACL (Access Control Lists), 177
 modifying, 198–199
 named extended IPv4 ACL, 212–216
 named standard IPv4 ACL, 189–190, 193–195
NAT (Network Address Translation), 226, 237
 advantages of, 238, 261
 characteristics of, 227–231
 configuring, 260
 defined, 227–228
 disadvantages of, 238–239, 261

- dynamic NAT, 232–233, 244, 245–247, 249–251, 260–261
 - analyzing*, 247–249
 - configuring*, 251
 - topologies*, 244–245
- global NAT addresses, 229–231
- inside global NAT addresses, 230
- inside local NAT addresses, 230–231
- inside NAT addresses, 229–231
- local NAT addresses, 229–231
- NAT overload. *See* PAT
- NAT64, 258–259
- NAT-PT, 259
- operation of, 228–229
- outside global NAT addresses, 231
- outside local NAT addresses, 231
- outside NAT addresses, 229, 231
- PAT, 233–234, 251, 260–261
 - analyzing*, 254–255
 - configuring*, 252–253
 - NAT comparisons*, 236–237
 - next available port*, 233–234
 - source port assignments*, 235
 - verifying*, 256–257
- pools, 245–247
- private IPv4 addresses, 226–227
- routers, private/public IPv4 address translations, 227
- static NAT, 231–232, 239–240, 242–244, 260–261
 - analyzing*, 241–242
 - configuring*, 240–241
 - topology*, 240
- stub networks, 228
- terminology, 229–231
- troubleshooting, 542–543
- NBAR (Network Based Application Recognition)**, 372
- NBMA (Non-Broadcast Multiaccess) networks**, 70
- NCS 6000 series routers**, 489
- neighbor adjacencies**
 - establishing, 18–20
 - OSPF link-state operation, 6
 - troubleshooting, 539
- neighbor tables (IPv6)**, 554–555
- neighbors**, list of, 17
- NETCONF**, 638–639
- network addresses**, prefixes, 12
- Network Analysis Module (NAM)**, 528
- network analyzers (portable)**, 528
- network command**, point-to-point OSPF networks
 - command syntax, 40
 - configuring OSPF, 41–43
- network edge routers**, 488–489
- network layer**, troubleshooting, 537–539
- network masks**, hello packets, 16
- networks**
 - ACL, 164, 165, 175, 188
 - ACE*, 164–165
 - best practices*, 174–175
 - creating*, 173–175, 183, 188
 - defined*, 164
 - extended ACL*, 175–176, 180–181, 203–206, 207–218, 220
 - implicit denies*, 167, 182
 - limits per interface*, 173–174
 - modifying*, 195–196, 219
 - modifying, sequence numbers method*, 197–198
 - modifying with text method*, 196–197
 - named ACL*, 177, 189–190, 193–195, 198–199, 212–216
 - numbered ACL*, 176, 188–189, 191–193, 195, 204–206, 209–210
 - packet filtering*, 164–168
 - placement of*, 177–181
 - purpose of*, 164–168, 182
 - standard ACL*, 175–176, 179, 190, 200–203, 219–220
 - stateful firewall services*, 210, 220
 - statistics*, 199
 - types of*, 175–181, 183–184
 - wildcard masks*, 168–173, 182–183
 - ATM, 296, 324
 - attacks, 109, 117, 158. *See also* security
 - access attacks*, 110–113
 - address spoofing attacks*, 118, 120–121
 - amplification attacks*, 118–120
 - ARP vulnerabilities/attacks*, 127–130
 - baiting attacks*, 114
 - best practices*, 137–143, 159
 - buffer overflow attacks*, 112–113
 - DDoS attacks*, 116–117
 - DHCP attacks*, 134–136
 - DNS attacks*, 131–133

- DoS attacks*, 115–116
- dumpster diving attacks*, 114
- ICMP attacks*, 117–119
- impersonation attacks*, 114
- IP attacks*, 117–122
- IP service attacks*, 127–136
- MITM attacks*, 112–113, 118
- password attacks*, 111
- phishing attacks* 114. *See also spear phishing attacks*
- port redirection attacks*, 112
- pretexting attacks*, 114
- reconnaissance attacks*, 109–110
- reflection attacks*, 118–120
- session hijacking attacks*, 118
- shoulder surfing attacks*, 114
- social engineering attacks*, 114–115
- something for something (quid pro quo) attacks*, 114
- spam attacks*, 114
- spear phishing attacks*, 114. *See also phishing attacks*
- spoofing attacks*, 111
- tailgating attacks*, 114
- TCP vulnerabilities/attacks*, 122–126, 158
- trust exploitation attacks*, 111
- UDP vulnerabilities/attacks*, 122, 126–127, 158
- vectors of, 96–97
 - zombies*, 116
- automation, 619, 641, 651
 - API*, 628–639, 651–652
 - benefits of*, 619, 620
 - Cisco DNA*, 647–648
 - Cisco DNA Center*, 648–650, 652
 - concept of*, 620–621
 - configuration management tools*, 639–643, 652
 - data formats*, 620–628
 - IBN*, 644–646, 652
 - JSON*, 622–626, 632–633
 - smart devices*, 620
 - XML*, 623, 627–628
 - YAML*, 623, 626–627
- backbone networks, 287
- backhaul networks, 287
- bandwidth, 354
- baselines, 408, 507–509, 524
- borderless switched networks, 458–461
- bottlenecks/congestion, troubleshooting, 532
- branch networks, 281
- broadcast multiaccess networks, 49, 84
- campus networks, 280
- Cisco DNA, 647–648
- Cisco DNA Assurance, 648
- Cisco DNA Center, 648–650, 652
- Cisco DNA Security, 648
- CLI, 639
- communications
 - ATM*, 296, 324
 - circuit-switched network communications*, 290
 - demodulation*, 288, 295
 - DWDM multiplexing*, 292
 - Frame Relay networks*, 295–296
 - jitter*, 291, 294, 355
 - latency*, 291, 294, 302, 314
 - modulation*, 288, 295
 - packet-switched network communications*, 290–291, 295–296
 - parallel network communications*, 289
 - SDH cabling standard*, 291–292
 - serial network communications*, 289
 - SONET cabling standard*, 291–292
- configuring
 - CLI, 639
 - SNMP, 640–641
- congestion, 353–354
- converged networks, 458, 493
- data link layer, troubleshooting, 534–537
- delays, 353
 - code delays*, 355
 - data delays*, 360–361
 - de-jitter delays*, 355
 - fixed delays*, 355
 - jitter*, 291, 294, 355
 - packetization delays*, 355
 - propagation delays*, 355
 - queuing delays*, 355
 - serialization delays*, 355
 - variable delays*, 355
- designing, 455
 - borderless switched networks*, 458–461
 - collapsed core network design*, 464
 - hierarchical networks*, 455–465, 475

- line cards*, 480, 482
- routers*, 487–492
- scalable networks*, 455–458, 465–477
- SFP devices*, 482
- switch hardware*, 477–487
- three-tier network design*, 455, 460, 463
- two-tier network design*, 461, 464
- distributed networks, 282
- documentation, 502, 572
 - baselines*, 507–509
 - data measurement*, 510–512
 - device documentation*, 505–507, 512
 - logical network topologies*, 504–505
 - overview of*, 502
 - physical network topologies*, 503
- enterprise networks, 458, 477, 487, 491, 493, 494
- Ethernet networks, adjacencies, 23–24
- evolution of, 279–282
- firewalls, 139–140
- Frame Relay networks, 295–296
- hacking tools, 103
- HFC networks, cable modems, 305
- hierarchical networks, 493
 - access layer*, 462, 475
 - borderless switched networks*, 458–461
 - core layer*, 462
 - distribution layer*, 462
 - distribution layer switches*, 461, 462, 493
 - OSPF, 476–477
 - scalability*, 455–458
 - switched networks*, 464–465
 - three-tier network design*, 455, 460, 463
 - two-tier network design*, 461, 464
- IBN, 644–646, 652
- ISDN, 295
- knowledge bases, 524
- LAN
 - campus LAN switches*, 477–478
 - WAN comparisons*, 272–273
- line cards*, 480, 482
- local network addressing, verifying, 553–556
- managing, 390
 - backing up configurations*, 428–430, 436
 - calendar services*, 400
 - CDP, 390–396, 443
 - changing passwords*, 435
 - IOS images*, 424, 437–442
 - LLDP, 396–400, 443
 - NTP, 400–405, 443–444
 - password recovery*, 433–436, 437
 - restoring configurations from text files*, 428–430
 - router configurations*, 431–432
 - router file systems*, 423–424, 445–446
 - routers, USB ports*, 430–432
 - SNMP, 405–418, 444
 - switch file systems*, 426–427, 445–446
 - Syslog, 418–423, 444–445
 - time services*, 400
 - USB drives*, 430–432
- multiaccess OSPF networks, 49–51
- NBMA, 70
- network layer, troubleshooting, 537–539
- NMS
 - SNMP, 405, 444
 - tools*, 524
- NOC, 457
- OSPF, network types, 84–85
- paths, verifying, 562–566
- physical layer
 - troubleshooting*, 531–534
 - verifying*, 549–551
- point-to-point OSPF networks, 40, 83–84
 - area ID*, 40
 - configuring*, 49
 - configuring with ipospf command*, 43–44
 - configuring with network command*, 41–43
 - ipospf command*, 43–44
 - loopback interfaces*, 48
 - network command*, 40, 41–43
 - passive interfaces*, 44–46
 - verifying network type*, 46–48
 - wildcard masks*, 40, 41, 42–43
- prioritizing traffic, 353–354
- PSTN, 295
- router hardware, 487–492
- routers, 494–495
- scalable networks, 493–494
 - designing*, 465–477
 - hierarchical networks*, 455–458
- scanning tools, 103
- SD-Access, 647
- SDN, 595, 598, 600, 610–611

- ACI, 598, 602–603
- CEF, 596
- central controller, 597
- control plane, 595
- controller-based SDN, 605, 611–612
- controllers, 600–602
- data plane, 596
- device-based SDN, 604–605
- framework, 599
- Layer 3 switches, 596
- management plane, 598
- OpenFlow, 598
- OpenStack, 598
- policy-based SDN, 605
- traditional architectures and, 599
- SD-WAN, 648
- security, 95, 157. *See also* attacks; VPN
 - adware, 108
 - ASA, 140
 - assets, 96
 - attack tools, 101–102
 - attack types, 104–105
 - availability, 138
 - best practices, 137–143
 - blacklisting URL, 142
 - breaches, 95
 - confidentiality, 138
 - content security appliances, 141–143
 - cryptography, 143–146, 159
 - cybercriminals, 95, 100
 - cybersecurity, current state of, 95–98
 - data confidentiality, 144, 150
 - data integrity, 144, 145
 - data nonrepudiation, 144
 - debuggers, 104
 - defense-in-depth approach, 138–139
 - encryption, 104, 151–156
 - ESA, 142
 - ethical hacking, 95
 - evolution of tools, 102–104
 - exploits, 96
 - firewalls, 139–140
 - forensic tools, 103
 - fuzzers, 103
 - hackers, 98–100
 - backing OS, 104
 - backing tools, 103
 - hacktivists, 100
 - bash functions, 144–147
 - IDS, 140–141
 - integrity, 138
 - IPS, 140–141
 - layered approach, 138–139
 - malware, 106–109
 - mitigation, 96
 - origin authentication, 144, 147–149
 - packet crafting tools, 103
 - packet sniffers, 103
 - password crackers, 103
 - penetration testing tools, 102–104
 - ransomware, 108
 - risk, 96
 - rootkit detectors, 103
 - rootkits, 108
 - scanning tools, 103
 - script kiddies, 100
 - spyware, 108
 - threat actors, 98–101, 157
 - threats, 96
 - Trojan horses, 106, 107
 - URL filtering, 142
 - vectors of data loss, 97–98
 - vectors of network attacks, 96–97
 - viruses, 106–107
 - vulnerabilities, 96
 - vulnerability brokers, 100
 - vulnerability exploitation tools, 104
 - vulnerability scanners, 104
 - wireless backing tools, 103
 - worms, 106, 108
 - WSA, 142–143
- SFP devices, 482
- small networks, 279–280
- SNMP, 640–641
- stub networks, NAT and, 228
- switch hardware, 477–487
- switched networks, borderless switched networks,
 - 458–461, 464–465
- switches, 481, 494–495
- toll networks, 286
- topologies
 - logical network topologies, 504–505
 - physical network topologies, 503

- traffic
 - data traffic*, 357, 360–361
 - video traffic*, 357–360
 - voice traffic*, 357–358
- transmission quality, 353, 382
 - congestion*, 353–354
 - delays*, 353, 355
 - packet loss*, 355–357
 - prioritizing traffic*, 353–354
- troubleshooting
 - analyzing information*, 514
 - application layer*, 543–545
 - bottom-up troubleshooting method*, 518–519
 - buffered logging*, 529
 - comparison troubleshooting method*, 522
 - console logging*, 529
 - data link layer*, 534–537
 - defining problems*, 514
 - divide-and-conquer troubleshooting method*, 520–521
 - documentation*, 502–512, 572
 - educated guess troubleshooting method*, 522
 - eliminating probable cause*, 514
 - flowcharts*, 512–513
 - follow-the-path troubleshooting method*, 521–522
 - gathering information*, 514, 516–517
 - general troubleshooting procedures*, 512–513
 - hardware troubleshooting tools*, 525–528
 - IP connectivity*, 574–576
 - layered models*, 517–518
 - network layer*, 537–539
 - physical layer*, 531–534
 - process of*, 512–523
 - proposing hypotheses*, 514
 - protocol analyzers*, 525
 - questioning end users*, 515–516
 - selecting troubleshooting method*, 523
 - seven-step troubleshooting process*, 513–515
 - SNMP traps*, 530
 - software troubleshooting tools*, 524
 - solving problems*, 515
 - structured troubleshooting methods*, 518–522
 - substitution troubleshooting method*, 522
 - symptoms/causes of network problems*, 531–545, 573–574
 - terminal lines*, 529
 - testing hypotheses*, 515
 - top-down troubleshooting method*, 519–520
- virtual networks, 592–593
 - complexity of*, 594–595, 610
 - switches*, 479
 - UCS Manager*, 593–594
- virtualization, 583, 609
 - abstraction layers*, 589–590
 - advantages of*, 589
 - AWA Management Console*, 586
 - cloud computing*, 583–586
 - dedicated servers*, 586–587
 - disaster recovery*, 589
 - hypervisors*, 588, 591–593
 - legacy support*, 589
 - prototyping*, 589
 - SDN*, 595–598, 610–611
 - servers*, 587–589
 - virtual network infrastructure*, 592–595, 610
- VLAN, 556–558, 594
- VNI, 357
- VPN, 283, 308, 321, 344. *See also* IPsec
 - AnyConnect Secure Mobility Client*, 321
 - ASA*, 321
 - authentication*, 339–342
 - benefits of*, 322–323
 - client-based VPN*, 321, 326
 - clientless VPN*, 326
 - cost metrics*, 322
 - data integrity*, 338–339
 - digital certificates*, 327, 333, 335, 339, 341–342, 344–345
 - DMVPN*, 330–331
 - enterprise VPN*, 324–325
 - GRE over IPsec*, 328–329
 - MPLS VPN*, 332
 - PKI*, 327, 344
 - remote access VPN*, 283, 308, 312, 314–315, 324, 325–326
 - scalability*, 323
 - service provider VPN*, 324–325
 - site-to-site VPN*, 283, 308, 312, 314–315, 323, 327–328
 - SOHO*, 321
 - SSL VPN*, 326–327
 - VTI*, 331–332

- VRF, 595
- WAN
 - 3G/4G/5G, 302, 307, 314
 - AP, 288
 - ATM, 296, 324
 - backbone networks, 287
 - backhaul networks, 287
 - branch networks, 281
 - cable Internet connectivity, 305–306
 - cable modems, 288
 - campus networks, 280
 - circuit-switched network communications, 290
 - circuit-switched WAN connectivity, 295
 - CO, 286
 - connectivity, 292–301
 - core devices, 288
 - CPE, 286
 - CSU, 288
 - DCE, 286–288
 - dedicated broadband WAN connectivity, 297–298
 - demarcation points, 286
 - devices, 287–289
 - distributed networks, 282
 - DSL Internet connectivity, 302–304
 - DSL modems, 288
 - DSU, 288
 - DTE, 286–288
 - DWDM multiplexing, 292
 - E-carriers, 294
 - Frame Relay networks, 295–296
 - Internet-based broadband WAN connectivity, 298, 301–311, 314–315
 - ISDN, 295
 - ISP Internet connectivity, 309–310
 - LAN comparisons, 272–273
 - leased-line WAN connectivity, 293–294
 - local loops (last mile), 286
 - LTE, 307
 - Metro Ethernet WAN connectivity, 298–300, 332
 - modern WAN connectivity, 296–301, 314
 - MPLS, 298, 300–301, 324, 332
 - operation of, 283–292, 312–313
 - optical converters, 288
 - OSI model, 284–285
 - packet-switched network communications, 290–291, 295–296
 - packet-switched WAN connectivity, 298
 - parallel network communications, 289
 - POP, 286
 - private WAN, 273
 - PSTN, 295
 - public WAN, 273
 - purpose of, 272–282, 312
 - SDH cabling standard, 291–292
 - serial network communications, 289
 - small networks, 279–280
 - SONET cabling standard, 291–292
 - standards, 283
 - T-carriers, 294
 - teleworking, 283, 302, 308, 312, 314
 - terminology, 285–287
 - toll networks, 286
 - topologies, 274–277
 - traditional WAN connectivity, 292–296, 312–313
 - voiceband modems, 288
 - wired Internet connectivity, 301–302
 - wireless Internet connectivity, 302
 - wireless Internet-based broadband connectivity, 306–307
 - wireless routers, 288
- next available port (PAT), 235–236
- Nexus 9000 series switches, 602
- NFS (Network File System), 544
- NMS (Network Management System)
 - SNMP, 405, 444
 - agent traps, 408–409
 - community strings, 412–415
 - MIB OID, 415
 - Object Navigator, 417–418
 - operation of, 406–407
 - snmpget utility, 417
 - tools, 524
- NOC (Network Operations Center), 457
- noise, troubleshooting, 534
- nonrepudiation of data, 144
- NTP (Network Time Protocol), 400, 443–444
 - authoritative time sources, 401–402, 443–444
 - calendar services, 400
 - client topologies, 402–403
 - configuring, 402–405
 - operation of, 401–402

- server topologies, 402–403
- strata, 401–402
- stratum, 401–405, 443–444
- time services, 400
- verifying, 403–405
- numbered ACL (Access Control Lists), 176**
 - numbered extended IPv4 ACL, 204–206, 209–210
 - numbered standard IPv4 ACL, 188–189, 191–193, 195
- NVRAM, file systems, 425–426**

O

- Object Navigator (SNMP), 417–418**
- OC (Optical Carriers), 294**
- OID (Object ID), MIB OID, 415**
- open (public) API, 631–632**
- open resolver attacks (DNS), 131**
- OpenFlow, 598**
- OpenStack, 598**
- optical converters, 288**
- optical fiber Internet connectivity, 305–306**
- optical nodes, 305**
- Optical Time-Domain Reflectometers (OTDR), 527**
- order of precedence, router ID, 36–37**
- origin authentication, 144**
 - HMAC, 147–149
 - IPsec, 333, 335
- OS (Operating Systems), hacking, 104**
- OSI model**
 - common devices, 517–518
 - WAN, 284–285
- OSPF (Open Shortest Path First), 17**
 - adjacencies, 23–24
 - algorithms, 5
 - BDR
 - adjacencies, 51, 54–56*
 - election process, 20, 23–24, 56–59*
 - multiaccess OSPF networks, 49–51, 53, 56–59*
 - router priorities, 61–63*
 - components of, 4–5
 - data structures, 4–5
 - databases, 5, 20–22
 - Down state, 17, 18–19
 - DR
 - election process, 56–59*
 - failures/recovery, 58–59*
 - multiaccess OSPF networks, 49–51, 53–54, 56–59*
 - router priorities, 61–63*
 - DR election, 20, 23–24
 - Exchange state, 18
 - ExStart state, 18
 - Full state, 18
 - hierarchical networks, 476–477
 - Init state, 17–19
 - introduction to, 3
 - link-state operation, 6
 - establishing neighbor adjacencies, 6*
 - LSA, 6–7*
 - LSDB, 7*
 - route selection, 8–9*
 - SPF algorithms, 8–9*
 - SPF trees, 8–9*
 - Loading state, 18
 - LSA
 - BDR, 24–26*
 - DR, 24–26*
 - flooding, 23–24*
 - multiaccess OSPF networks, 49
 - adjacencies, 54–56*
 - designated routers, 49–51*
 - reference topologies, 51–52, 57*
 - router election process, 56–59*
 - router priorities, 61–63*
 - verifying router roles, 52–54*
 - multi-area OSPF, 9–11
 - neighbor adjacencies, 6, 18–20
 - network types, 84–85
 - operational states, 17–18
 - OSPFv2, 12
 - OSPFv3, 12–13
 - OSPFv4, 12
 - overview of, 3
 - packets, 4, 13–14, 17
 - hello packets, 15–17*
 - LSU packets, 14*
 - point-to-point OSPF networks, 40, 83–84
 - area ID, 40*
 - configuring, 49*
 - configuring with ipospf command, 43–44*
 - configuring with network command, 41–43*

- ipospf command*, 43–44
 - loopback interfaces*, 48
 - network command*, 40, 41–43
 - passive interfaces*, 44–46
 - verifying network type*, 46–48
 - wildcard masks*, 40–43
 - routers
 - configuration mode*, 35
 - convergence*, 6, 17–26
 - designated routers*, 49–51
 - ID*, 34–40, 83
 - routing protocol messages, 4
 - single-area OSPF, 9, 10, 34, 38
 - cost metrics*, 63–67
 - dead intervals*, 70–73
 - default route propagation*, 73–77, 86
 - hello packet intervals*, 69–73
 - modifying*, 85–86
 - point-to-point OSPF networks*, 40–49
 - reference bandwidth adjustments*, 64–66
 - reference topologies*, 34–35
 - router ID*, 34–40
 - static routes*, 73–77
 - test failover to backup routes*, 69
 - verifying*, 77–82, 86–87
 - Two-Way state, 18, 19–20
 - OTDR (Optical Time-Domain Reflectometers), 527
 - outbound ACL filters, 167
 - output errors, troubleshooting, 551
 - output queue drops, 550
 - outside global NAT addresses, 231
 - outside local NAT addresses, 231
 - outside NAT addresses, 229, 231
- P**
-
- packetization delays, 355
 - packets
 - crafting tools, 103
 - DBD packets, 13–14, 21–22
 - filtering, 164–166
 - hello packets, 13–14, 15–17
 - ingress packets, 372
 - IPv4 packet headers, 374–375
 - IPv6 packet headers, 374–375
 - loss, 355–357, 371
 - LSAck packets, 13–14
 - LSR packets, 13–14, 22
 - LSU packets, 13–14
 - OSPF packets, 4, 13–17
 - queuing. *See* delay
 - sniffers, 103
 - packet-switched network communications, 290–291
 - ATM, 296, 324
 - Frame Relay networks, 295–296
 - packet-switched WAN connectivity, 298
 - parallel network communications, 289
 - partially meshed WAN topology, 277
 - partner API, 632
 - passive interfaces, point-to-point OSPF networks, 44–46
 - passwords
 - attacks, 105, 111
 - changing, 435
 - configuration register, 433–435, 437
 - password crackers, 103
 - plaintext passwords, 415
 - recovery, 433–436, 437
 - ROMMON mode, 433–434
 - PAT (Port Address Translation), 233–234, 251, 260–261
 - analyzing, 254–255
 - configuring
 - address pools*, 253
 - single IP addresses*, 252
 - NAT comparisons, 236–237
 - next available port, 233–234
 - source port assignments, 235
 - verifying, 256–257
 - paths (network), verifying, 562–566
 - penetration testing tools, 102–104
 - performance, troubleshooting, 532, 535
 - phishing attacks, 114. *See also* spear phishing attacks
 - physical layer (networks)
 - troubleshooting, 531–534
 - verifying, 549–551
 - physical network topologies, 503
 - pinging, 532, 534
 - gathering information (troubleshooting process), 517
 - IPv4, 547–548
 - IPv6, 548–549
 - TFTP servers, 438, 440

- PKI (Public Key Infrastructure), 327, 344
 - plaintext passwords, 415
 - playout delay buffers, 355–356
 - PoE (Power over Ethernet), switches, 484–486
 - point-to-point OSPF networks, 40, 83–84
 - area ID, 40
 - configuring, 49
 - ipospf command*, 43–44
 - network command*, 41–43
 - ipospf command*, configuring OSPF, 43–44
 - loopback interfaces, 48
 - network command
 - configuring OSPF*, 41–43
 - syntax*, 40
 - passive interfaces, 44–46
 - verifying network type, 46–48
 - wildcard masks, 40–43
 - point-to-point WAN topology, 274–275
 - policing traffic, QoS, 380–381
 - policy-based SDN, 605
 - polling scenarios, SNMP, 415–417
 - POP (Point of Presence), 286, 312, 544
 - portable network analyzers, 528
 - ports
 - density, switches, 482, 486
 - destination ports, troubleshooting, 541
 - next available port (PAT), 235–236
 - redirection attacks, 112
 - source ports
 - assigning*, 235
 - troubleshooting*, 541
 - speeds, switches, 487
 - USB ports on routers, 430
 - VTY port security, standard IPv4 ACL, 200–203, 220
 - wire speeds, 483
 - Postman, 638
 - power supplies, troubleshooting, 533
 - PPP (Point-to-Point Protocol), DSL Internet connectivity, 303–304
 - precedence (router ID), order of, 36–37
 - prefixes, 12
 - pretexting attacks, 114
 - PRI (Priority) fields, 373
 - Prime NAM (Network Analysis Module), 528
 - prioritizing network traffic, 353–354
 - private (internal) API, 632
 - private clouds, 584
 - private IPv4 addresses, 226–227
 - private WAN (Wide-Area Networks), 273
 - probable cause (troubleshooting process), eliminating, 514
 - problems (troubleshooting process)
 - defining, 514
 - solving, 515
 - program viruses, 107
 - propagating
 - delays, 355
 - static routes
 - default route propagation*, 73–77, 86
 - single-area OSPF*, 73–77
 - proposing hypotheses (troubleshooting process), 514
 - protocols
 - analyzers, 525
 - encapsulation (IPsec), 336
 - prototyping, virtualization, 589
 - proxy Trojan horses, 107
 - PSK (Pre-Shared Keys), 339–340
 - PSTN (Public Service Telephone Networks), 295
 - public clouds, 584
 - public key algorithms, 152–156
 - public (open) API, 631–632
 - public WAN (Wide-Area Networks), 273
 - Puppet, 643
 - PVC (Permanent Virtual Circuits), 295–296
 - Python, 638
-
- ## Q
-
- QoS (Quality of Service)
 - classification/marketing tools, 371–372
 - congestion
 - avoidance tools*, 371, 379–380
 - management tools, 371, 379–380
 - DSP, 357
 - egress packets, 372
 - implementation techniques, 384–385
 - ingress packets, 372
 - IPP, 373, 375, 377–378
 - models, 383–384
 - network traffic
 - data traffic*, 357, 360–361

- video traffic*, 357–360
- voice traffic*, 357, 358
- network transmissions, 353, 382
 - congestion*, 353–354
 - delays*, 353, 355
 - packet loss*, 355–357
 - prioritizing traffic*, 353–354
- packet loss, avoiding, 371
- playout delay buffers, 355–356
- policy guidelines, 381
- policy models
 - best-effort QoS policy model*, 366–367
 - DiffServ*, 366, 369–370
 - IntServ*, 366–368
 - selecting*, 366
- queueing algorithms, 361, 383
 - CBWFQ, 364
 - FIFO, 362
 - LLQ, 365
 - WFQ, 362–364
- RSVP, 368, 370
- tool usage, sequence of, 372
- ToS values, 363, 374–375, 377, 383
- traffic
 - characteristics*, 382–383
 - classification*, 362–363, 368
 - marking*, 372–379, 382–383
 - policing*, 380–381
 - shaping*, 380–381
- WRED, 371
- questioning end users (troubleshooting process), 515–516
- queue drops
 - input queue drops, 550
 - output queue drops, 550
- queueing algorithms (QoS), 383
 - CBWFQ, 364
 - FIFO, 362
 - LLQ, 365
 - overview of, 361
 - WFQ, 362–364
- queueing delays, 355
- queueing packets. *See* delay
- quid pro quo (something for something) attacks, 114

R

- rack units (RU), 481, 494
- ransomware, 108
- RC (Rivest Cipher) series algorithms, 152
- reconnaissance attacks, 109–110
- recovery, passwords, 433–437
- redundancy
 - network design, 469
 - scalable networks, 469
- redundant links, scalable networks, 466–467
- reference bandwidths, single-area OSPF, 64–66
- reference topologies
 - end-to-end IP connectivity, troubleshooting, 545–547
 - multiaccess OSPF networks, 51–52, 57
 - single-area OSPF, 34–35, 38, 74
- reflection attacks, 118–120
- rejoins, routers, multiaccess OSPF networks, 58–59
- reliability, switches, 486
- remote access Trojan horses, 107
- remote access VPN (Virtual Private Networks), 283, 308, 312, 314–315, 324–326
- removable media, data loss, 98
- reset attacks (TCP), 125–126
- resiliency, borderless switched networks, 459
- REST (Representational State Transfer), 632–639, 651–652
- RESTful API, 633–639
- restoring configurations
 - router configurations, 432
 - from text files, 428–430
- rid values, 37
- risk (security), defined, 96
- rogue DHCP servers, 121, 134–136
- ROMMON mode, 433–434
- rootkit detectors, 103
- rootkits, 108
- routers, 494–495
 - 800 series routers, 492
 - 900 series routers, 490
 - 5500 series routers, 491
 - ASBR, 74
 - ASR 1000 series routers, 490–491
 - ASR 9000 series routers, 488–491
 - BDR, 17

- election in OSPF*, 20, 23–24
- LSA*, 24–26
- multiaccess OSPF networks*, 49–51, 53, 56–59
- branch routers, 488
- configurations
 - copying*, 431
 - restoring*, 432
 - saving*, 435
 - verifying*, 432
- convergence, 6, 17–26
- DBD packets, 21–22
- device documentation, 505–506
- Dijkstra’s algorithm, 5
- DR, 16
 - election in OSPF*, 20, 23–24
 - failures/recovery*, 58–59
 - LSA*, 24–26
 - multiaccess OSPF networks*, 49–51, 53–54, 56–59
 - router ID*, 36
- DROTHER, 50–53
- edge routers, 74, 470–471, 488–489
- failover tests to backup routes, single-area OSPF, 69
- file systems, 423–424, 445–446
 - Flash file systems*, 425
 - NVRAM file systems*, 425–426
- fixed configuration routers, 492
- form factors, 490–492
- hub routers, 275–276
- ID, 16, 34, 40, 83
 - assigning*, 40
 - choosing*, 36–37
 - configuration mode*, 35
 - configuring*, 38–39
 - DR election*, 36
 - loopback interfaces*, 37–38
 - modifying*, 39–40
 - order of precedence*, 36–37
 - reference topologies*, 34–35
 - rid values*, 37
 - synchronization of OSPF databases*, 36
 - verifying*, 38–39
- industrial routers, 490, 492
- ISR 4000 series routers, 488
- list of neighbors, 17
- LSR, 300–301
 - LSR packets, 22
 - modular routers, 492
 - MPLS routers, 300–301
 - NAT routers, private/public IPv4 address translations, 227
 - NCS 6000 series routers, 489
 - network edge routers, 488–489
 - OSPF
 - database synchronization*, 20–21
 - designated routers*, 49–51
 - priorities, 16, 61–63
 - requirements, 487–488
 - service provider routers, 489
 - software clock, setting manually, 400
 - SPF algorithms, 10–11
 - spoke routers, 275–276
 - USB ports, 430
 - wireless routers, 288
- routing**
 - GRE
 - GRE over IPsec*, 328–329
 - mGRE*, 330–331
 - OSPF
 - default route propagation*, 73–77, 86
 - link-state operation, route selection*, 8–9
 - protocols
 - failover tests to backup routes, single-area OSPF*, 69
 - link-state routing protocols. See OSPF messages*, 4
 - scalable routing protocol, 467–468
 - show ip route command, 517
 - show ipv6 route command, 517
 - tables, troubleshooting, 539
 - tuning protocols, scalable networks, 476–477
 - VRF, 595
- RPC (Remote Procedure Calls)**
 - JSON-RPC, 632
 - XML-RPC, 632
- RSA (Rivest, Shamir, Adleman)**
 - authentication, 340–342
 - encryption algorithms, 154
- RSVP (Resource Reservation Protocol)**, 368, 370
- RU (Rack Units)**, 481, 494
- Ruby**, 643

S

- SA (Security Associations), 334–335
- SaaS (Software as a Service), 584
- SaltStack, 643
- satellite Internet connectivity, 307
- saving router configurations, 435
- scalability
 - switches, 487
 - VPN, 323
- scalable networks, 493–494
 - designing, 465–466, 477
 - access layer*, 475
 - bandwidth*, 474–475
 - failure domains*, 469–474
 - multiple links*, 466–467
 - redundancy plans*, 469
 - redundant links*, 466–467
 - scalable routing protocol*, 467–468
 - tuning routing protocols*, 476–477
 - wireless connectivity*, 468
 - hierarchical networks, 455–458
- scalable routing protocol, 467–468
- scanning tools, 103–104
- script kiddies, 100
- script viruses, 107
- SD-Access, 647
- SDH cabling standard, 291–292
- SDN (Software-Defined Networking), 595, 598, 600, 610–611
 - ACI, 598, 602
 - ANP*, 602
 - APIC*, 602–603
 - APIC-EM*, 606–608
 - Nexus 9000 series switches*, 602
 - spine-leaf topologies*, 603
 - CEF, 596
 - central controller, 597
 - control plane, 595
 - controller-based SDN, 605, 611–612
 - controllers, 600–602
 - data plane, 596
 - device-based SDN, 604–605
 - framework, 599
 - Layer 3 switches, 596
 - management plane, 598
 - OpenFlow, 598
 - OpenStack, 598
 - policy-based SDN, 605
 - traditional architectures and, 599
- SD-WAN, 648
- SEAL (Software-Optimized Encryption Algorithm), 152, 338
- security. *See also* VPN
 - AnyConnect Secure Mobility Client, 321
 - ASA, 140, 321
 - attack tools, 101–102
 - attack types, 104–105
 - authentication, 339–340
 - HMAC*, 338–339
 - MD5*, 339
 - PSK*, 339, 340
 - RSA*, 340–342
 - SHA*, 339
 - cryptography, 143, 156, 159
 - data confidentiality*, 144, 150
 - data integrity*, 144–145
 - data nonrepudiation*, 144
 - encryption*, 151–156
 - hash functions*, 144–147
 - origin authentication*, 144, 147–149
 - data confidentiality, 144, 150
 - data integrity, 144–145
 - data nonrepudiation, 144
 - encryption
 - 3DES*, 152, 338
 - AES*, 152, 338
 - asymmetric encryption*, 152–156
 - DES*, 152, 338
 - DH*, 154–156
 - DSA*, 154
 - DSS*, 154
 - ElGamal*, 154
 - elliptic curve cryptography*, 154
 - public key algorithms*, 152–156
 - RC series algorithms*, 152
 - RSA*, 154
 - SEAL*, 152, 338
 - symmetric encryption*, 151–152
 - ESA, 142
 - firewalls, 139–140, 210, 220
 - GRE over IPsec, 328–329

- hash functions, 144
 - MD5, 145
 - SHA, 146–147
- HMAC, 338–339
- IDS, 140–141
- IKE, 335
- IPS, 140–141
- IPsec, 333, 344–345. *See also* VPN
 - AH, 336
 - authentication, 339–342
 - confidentiality, 333–334, 336–338
 - data integrity, 333–335, 338–339
 - Diffie-Hellman key exchanges, 333–335, 342–343
 - ESP, 336
 - framework of, 334–335
 - GRE over IPsec, 328–329
 - protocol encapsulation, 336
 - SA, 334–335
 - SSL comparisons, 326–327
 - transport and tunnel mode, 343
 - VTI, 331–332
- keys, compromised-key attacks, 105
- malware, 106, 108–109, 157
 - adware, 108
 - overview of, 106
 - ransomware, 108
 - rootkits, 108
 - spyware, 108
 - Trojan horses, 106–107
 - viruses, 106–107
 - worms, 106, 108
- MD5, 339
- networks, 95, 109, 117, 158
 - access attacks, 110–113
 - address spoofing attacks, 118, 120–121
 - amplification attacks, 118–120
 - ARP vulnerabilities/attacks, 127–130
 - ASA, 140
 - assets, 96
 - availability, 138
 - baiting attacks, 114
 - best practices, 137–143, 159
 - blacklisting URL, 142
 - breaches, 95
 - buffer overflow attacks, 112–113
 - confidentiality, 138
 - content security appliances, 141–143
 - cybercriminals, 95
 - cybersecurity, current state of, 95–98
 - DDoS attacks, 116–117
 - defense-in-depth approach, 138–139
 - DHCP attacks, 134–136
 - DNS attacks, 131–133
 - DoS attacks, 115–116
 - dumpster diving attacks, 114
 - ethical hacking, 95
 - exploits, 96
 - firewalls, 139–140
 - ICMP attacks, 117–119
 - IDS, 140–141
 - impersonation attacks, 114
 - integrity, 138
 - IP attacks, 117–122
 - IP service attacks, 127–136
 - IPS, 140–141
 - layered approach, 138–139
 - mitigation, 96
 - MITM attacks, 112–113, 118
 - password attacks, 111
 - phishing attacks, 114. *See also* spear phishing attacks
 - port redirection attacks, 112
 - pretexting attacks, 114
 - reconnaissance attacks, 109–110
 - reflection attacks, 118–120
 - risk, 96
 - session hijacking attacks, 118
 - shoulder surfing attacks, 114
 - social engineering attacks, 114–115
 - something for something (*quid pro quo*) attacks, 114
 - spam attacks, 114
 - spear phishing attacks, 114. *See also* phishing attacks
 - spoofing attacks, 111
 - tailgating attacks, 114
 - TCP vulnerabilities/attacks, 122–126, 158
 - threats, 96
 - trust exploitation attacks, 111
 - UDP vulnerabilities/attacks, 122, 126–127, 158
 - URL filtering, 142
 - vectors of data loss, 97–98

- vectors of network attacks*, 96–97
- vulnerabilities*, 96
- zombies*, 116
- origin authentication, 144, 147–149
- passwords
 - changing*, 435
 - configuration register*, 433–437
 - recovery*, 433–437
 - ROMMON mode*, 433–434
- SA, 334–335
- SHA, 339
- software disablers, 107
- SSL
 - IPsec comparisons*, 326–327
 - SSL VPN*, 326
- stateful firewall services, 210, 220
- Syslog security levels, 421
- threat actors, 98, 157
 - attack tools*, 102–104
 - cybercriminals*, 100
 - backers*, 98, 100
 - hacktivists*, 100
 - script kiddies*, 100
 - vulnerability brokers*, 100
- TLS, VPN, 326
- tools
 - debuggers*, 104
 - encryption tools*, 104
 - evolution of*, 102–104
 - forensic tools*, 103
 - fuzzers*, 103
 - backing OS*, 104
 - backing tools*, 103
 - packet crafting tools*, 103
 - packet sniffers*, 103
 - password crackers*, 103
 - penetration testing tools*, 102–104
 - rootkit detectors*, 103
 - scanning tools*, 103
 - SET, 115
 - vulnerability exploitation tools*, 104
 - vulnerability scanners*, 104
 - wireless backing tools*, 103
- VTY ports, standard IPv4 ACL, 200–203, 220
- vulnerabilities
 - defined*, 96
 - exploitation tools*, 104
 - fuzzers*, 103
 - scanners*, 104
 - vulnerability brokers*, 100
- WSA, 142–143
- sequence numbers method, modifying ACL, 197–198
- serial network communications, 289
- serialization delays, 355
- servers
 - DHCP servers, rogue DHCP servers, 121, 134–136, 158
 - sprawl, 587, 609
 - Syslog server
 - messages*, 419
 - as troubleshooting tool*, 529–531
 - TFTP servers
 - backing up configurations from*, 428–430, 436
 - IOS image backups*, 437–442
 - pinging*, 438, 440
 - virtualization, 589
 - dedicated servers*, 586–587
 - examples of*, 587–588
- service providers. *See* ISP
- services
 - cloud services, 584
 - IaaS, 584
 - PaaS, 584
 - SaaS, 584
 - stateful firewall services, 210, 220
- session hijacking attacks, 118, 126
- SET (Social Engineering Toolkits), 115
- set operations (SNMP), 406–407
- seven-step troubleshooting process, 513–515
- severity levels (Syslog), 444–445, 530
- SFP (Small Form-Factor Pluggable) devices, 482
- SHA (Secure Hash Algorithm), 146–147, 339
- shaping traffic, QoS, 380–381
- shoulder surfing attacks, 114
- show interfaces command, 549–550
- show ip interface brief command, 517
- show ip route command, 517
- show ipv6 interface brief command, 517
- show ipv6 route command, 517
- single point of failure, 275, 278
- single-area OSPF, 9, 10, 34

- cost metrics, 63–64
 - accumulating costs*, 66–67
 - manually setting cost value*, 67–69
 - reference bandwidths*, 65
- dead intervals, 70–73
- default route propagation, 73–77, 86
- hello packet intervals, 69–73
- modifying, 85–86
- point-to-point OSPF networks, 40
 - area ID*, 40
 - configuring*, 49
 - configuring with ipospf command*, 43–44
 - configuring with network command*, 41–43
 - ipospf command*, 43–44
 - loopback interfaces*, 48
 - network command*, 40–43
 - passive interfaces*, 44–46
 - verifying network type*, 46–48
 - wildcard masks*, 40–43
- reference bandwidth adjustments, 64–66
- reference topologies, 34–35, 38
- router ID, 34, 40
 - assigning*, 40
 - choosing*, 36–37
 - configuration mode*, 35
 - configuring*, 38–39
 - DR election*, 36
 - loopback interfaces*, 37–38
 - modifying*, 39–40
 - order of precedence*, 36–37
 - reference topologies*, 34–35, 38
 - synchronization of OSPF databases*, 36
 - verifying*, 38–39
- routers, test failover to backup routes, 69
- verifying, 86–87
 - interface settings*, 81–82
 - neighbors*, 77–79
 - process information*, 80–81
 - protocol settings*, 79–80
- single-carrier WAN connections, 278
- single-homed ISP connectivity, 309
- site-to-site VPN (Virtual-Private Networks), 283, 308, 312, 314–315, 323–324, 327–328
- SLA (Service Level Agreements), 278
- small networks, 279–280
- smart devices, 620
- SMTP (Simple Mail Transfer Protocol), 544
- sniffer attacks, 105
- SNMP (Simple Network Management Protocol), 405, 444, 544, 640–641
 - agent traps, 408–409
 - agents, 406–409
 - community strings, 412–415
 - get operations, 406–407
 - messages, exchanging, 409
 - MIB OID, 415
 - NMS, 405
 - nodes, 405–406
 - Object Navigator, 417–418
 - operation of, 406–407
 - polling scenario, 415–417
 - set operations, 406–407
 - SNMP manager, 405–406, 407
 - snmpget utility, 417
 - traps, 530
 - troubleshooting, 543
 - versions of, 409–412
- SOAP (Simple Object Access Protocol), 632
- social engineering attacks, 114–115
- social networking, data loss, 98
- software
 - clock
 - displaying clock source*, 403
 - setting manually*, 400
 - security software disablers, 107
 - troubleshooting tools, 524
 - baselining tools*, 524
 - knowledge bases*, 524
 - NMS tools*, 524
 - protocol analyzers*, 525
- SOHO (Small Office, Home Office), VPN, 321
- solving problems (troubleshooting process), 515
- something for something (quid pro quo) attacks, 114
- SONET cabling standard, 291–292
- source ports
 - assigning, 235
 - troubleshooting, 541
- spam attacks, 114
- spear phishing attacks, 114. *See also* phishing attacks
- SPF (Shortest-Path First) algorithm, 5, 8–9, 10–11
- spine-leaf topologies, 603

- spoke routers, 275–276
- spoke-to-spoke tunnels, 331
- spoofing attacks, 105, 111
 - address spoofing attacks, 118, 120–121
 - ARP, 130
 - CAM tables, 121
 - DHCP, 134–136
 - MAC addresses, 120–121
- sprawl (servers), 587, 609
- spyware, 108
- SSH (Secure Shell), 544
- ssh -1 command, 517
- SSL (Secure Socket Layer)
 - IPsec comparisons, 326–327
 - VPN, 326–327
- stackable configuration switches, 481
- standard ACL (Access Control Lists), 166, 175, 175–176, 179, 190, 200–203, 219–220
- stateful firewall services, 210, 220
- state-sponsored hackers, 100
- static NAT (Network Address Translation), 231–232, 239–240, 260–261
 - analyzing, 241–242
 - configuring, 240–241
 - topology, 240
 - verifying, 242–244
- stealth attacks (DNS), 132
- storage devices (cloud), data loss, 98
- STP failures/loops, troubleshooting, 537
- stratum (NTP), 401–405, 443–444
- structured troubleshooting methods, 518
 - bottom-up troubleshooting method, 518–519
 - comparison troubleshooting method, 522
 - divide-and-conquer troubleshooting method, 520–521
 - educated guess troubleshooting method, 522
 - follow-the-path troubleshooting method, 521–522
 - selecting, 523
 - substitution troubleshooting method, 522
 - top-down troubleshooting method, 519–520
- stub networks, NAT, 228
- subnet masks, prefix lengths, 12
- substitution troubleshooting method, 522
- switch blocks, failure domains, 474
- switched networks, 464–465
- switches, 494–495
 - ASIC, 485–486
 - business considerations for switch selection, 486–487
 - campus LAN switches, 477–478
 - Catalyst 2960-C series switches, 485–486
 - Catalyst 3560-C series switches, 485
 - cloud-managed switches, 478
 - configuring
 - fixed configuration switches*, 480
 - modular configuration switches*, 480
 - stackable configuration switches*, 481
 - cost metrics, 486
 - data center switches, 478
 - device documentation, 506
 - distribution layer switches, 461, 462, 493
 - file systems, 426–427, 445–446
 - fixed configuration switches, 480
 - flow tables, 601
 - form factors, 479–481
 - forwarding rates, 483
 - frame buffers, 487
 - group tables, 602
 - LAN switches, device documentation, 506
 - Layer 3 switches, SDN, 596
 - MAC address tables, 555–557
 - meter tables, 602
 - modular configuration switches, 480
 - multilayer switching, 485–486
 - network design, 477–487
 - business considerations for switch selection*, 486–487
 - campus LAN switches*, 477–478
 - Catalyst 2960-C series switches*, 485–486
 - Catalyst 3560-C series switches*, 485
 - cloud-managed switches*, 478
 - data center switches*, 478
 - fixed configuration switches*, 480
 - forwarding rates*, 483
 - modular configuration switches*, 480
 - multilayer switching*, 485–486
 - platforms*, 477–479
 - PoE*, 484–485, 486
 - port density*, 482
 - service provider switches*, 479
 - stackable configuration switches*, 481
 - switch form factors*, 479–481

- thickness of switches*, 481
- virtual networks*, 479
- Nexus 9000 series switches, 602
- PoE, 484–486
- port density, 482, 486
- port speeds, 487
- reliability, 486
- RU, 481, 494
- scalability, 487
- service provider switches, 479
- stackable configuration switches, 481
- thickness of, 481
- virtual networks, 479
- wire speeds, 483
- symmetric encryption**, 151–152
- symptoms/causes of network problems**,
 - troubleshooting**, 573–574
 - data link layer, 534–537
 - physical layer, 531–534
- synchronizing OSPF databases**, 20–22
- syntax**
 - data formats, 622
 - JSON, 624–626
- Syslog**
 - configuring, 422–423
 - introduction to, 418–419
 - messages
 - destination of*, 420
 - facilities*, 422
 - format of*, 421
 - server messages*, 419
 - timestamps*, 422–423
 - operation of, 420
 - security levels, 421
 - severity levels, 444–445, 530
 - Syslog server as troubleshooting tool, 529–531
 - traps, configuring, 530–531
- headers**, 122
- reset attacks, 125–126
- services, 123
- session hijacking attacks, 126
- TCP-established extended ACL, 210–211
- TCP SYN flood attacks, 124
- vulnerabilities, 122–123, 158
- TDR (Time-Domain Reflectometers)**, 527
- teleworking**, 283, 302, 308, 312, 314
- telnet command**, 517, 544
- Tera Term**, configuration backups from TFTP servers, 427–428, 436
- terminal lines**, 529
- testing**
 - cable testers, 526–527
 - failover to backup routes, single-area OSPF, 69
 - hypotheses (troubleshooting process), 515
 - portable network analyzers, 528
 - Prime NAM, 528
- text files**, restoring configurations from, 428–430
- text method**, modifying ACL, 196–197
- TFTP (Trivial File Transfer Protocol)**, 544
 - backing up configurations from, 428–430, 436 servers
 - IOS image backups*, 437–442
 - pinging*, 438, 440
- thickness of switches**, 481
- threat actors (security)**, 98, 157
 - attack tools, 101–102
 - cybercriminals, 100
 - hackers, 98, 100
 - hacktivists, 100
 - script kiddies, 100
 - vulnerability brokers, 100
- threats (security)**, defined, 96
- three-tier network design**, 455, 460, 463
- time**, authoritative time sources, 401–402, 443–444
- time services**, network management, 400
- Time-Domain Reflectometers**. *See* TDR
- timestamps**, Syslog messages, 422–423
- TLS (Transport Layer Security)**, SSL VPN, 326
- toll networks**, 286
- tools (security)**
 - attack tools, 101–102
 - debuggers, 104
 - encryption tools, 104

T

- tailgating attacks**, 114
- Talos, ESA**, 142
- T-carriers**, 294
- TCI (Tag Control Information) fields**, 373
- TCP (Transmission Control Protocol)**
 - flow control, 123

- evolution of, 102–104
- forensic tools, 103
- fuzzers, 103
- hacking OS, 104
- hacking tools, 103
- packet crafting tools, 103
- packet sniffers, 103
- password crackers, 103
- penetration testing tools, 102–104
- rootkit detectors, 103
- scanning tools, 103
- SET, 115
- vulnerability exploitation tools, 104
- vulnerability scanners, 104
- wireless hacking tools, 103
- top-down troubleshooting method, 519–520**
- topologies**
 - databases, troubleshooting, 539
 - dynamic NAT, 244–245
 - hierarchical topologies, multi-area OSPF, 11
 - logical network topologies, 504–505
 - MPLS, 300
 - NAT terminology, 230
 - physical network topologies, 503
 - reference topologies
 - multiaccess OSPF networks, 51–52, 57*
 - single-area OSPF, 34–35, 38, 74*
 - troubleshooting end-to-end IP connectivity, 545–547*
 - spine-leaf topologies, 603
 - tables, LSDB, 7
 - VPN, 323
 - remote access VPN, 324*
 - site-to-site VPN, 327–328*
 - WAN, 274
 - dual-homed WAN topology, 276*
 - fully meshed WAN topology, 276*
 - hub-and-spoke WAN topology, 275, 330–331*
 - partially meshed WAN topology, 277*
 - point-to-point WAN topology, 274–275*
- ToS (Type of Service) values, 363, 374–375, 377, 383
- traceroute command, 517**
 - IPv4, 548
 - IPv6, 548–549
- traditional WAN connectivity, 292–296, 312–313**
- traffic (networks)**
 - classification, 362, 363, 368. *See also* classification/ marking tools
 - data traffic, 357, 360–361
 - flows
 - ACL, 165*
 - troubleshooting, 541*
 - marking, QoS, 373, 382–383
 - DSCP, 375–377*
 - Ethernet, 373*
 - IPv4, 373, 375*
 - IPv6, 373, 375*
 - Layer 2, 373–374*
 - Layer 3, 374–375*
 - MPLS, 373*
 - NBAR classifications, 372*
 - Traffic Class field (IPv6), 375*
 - trust boundaries, 378–379*
 - Type of Service field (IPv4), 375*
 - Wi-Fi (802.11), 373*
 - policing, QoS, 380–381
 - shaping, QoS, 380–381
 - video traffic, 357, 358–360
 - voice traffic, 357, 358
- Traffic Class field (IPv6), 375**
- transmission quality, networks, 353, 382**
 - congestion, 353, 354
 - delays, 353
 - code delays, 355*
 - data delays, 360–361*
 - de-jitter delays, 355*
 - fixed delays, 355*
 - jitter, 291, 294, 355*
 - packetization delays, 355*
 - propagation delays, 355*
 - queuing delays, 355*
 - serialization delays, 355*
 - variable delays, 355*
 - packet loss, 355–357
 - prioritizing traffic, 353–354
- transport and tunnel mode (IPsec), 343**
- transport layer**
 - troubleshooting
 - ACL, 539–542*
 - interoperability areas (common), 542–543*
 - NAT for IPv4, 542–543*
 - verifying, 566–567

transport protocols, 329

Trojan horses, 106, 107

troubleshooting

access control, 541

address mapping errors, 536

application layer, 543–545

attenuation, 533

BOOTP, 543

bottlenecks/congestion, 532

broadcasts, 536

cable analyzers, 527

cable testers, 526–527

cabling faults, 533

connectivity, 535, 539

connectivity, loss of, 532

console error messages, 533

console messages, 536

CPU overloads, 534

design limits, 534

destination ports, 541

DHCP, 543

DNS, 543

EMI, 534

encapsulation errors, 536

encryption protocols, 542, 543

end-to-end IP connectivity

components of, 545–547

duplex mismatches, 551–553

IPv4 ping, 547–548

IPv4 traceroute command, 548

IPv6 ping, 548–549

IPv6 traceroute command, 548–549

reference topologies, 545–547

verifying physical layer, 549–551

established keyword, 542

framing errors, 537

functionality, 535

general network issues, 539

hardware faults, 533

hardware troubleshooting tools

cable analyzers, 527

cable testers, 526–527

DMM, 525–526

portable network analyzers, 528

Prime NAM, 528

Syslog server, 529–531

high CPU utilization rates, 533

implicit denies, 541

input errors, 551

input queue drops, 550

interference, 534

interference configuration errors, 534

IP connectivity, 574–576

end-to-end connectivity, 545–549

local network addressing, 553–556

verifying ACL, 568–570

verifying default gateways, 558–562

verifying DNS, 570–571

verifying network paths, 562–566

verifying physical layer, 549–551

verifying transport layer, 566–567

VLAN assignments, 556–558

IPv4 addressing, 541

NAT for IPv4, 542–543

neighbor adjacencies, 539

networks

analyzing information, 514

application layer, 543–545

bottom-up troubleshooting, 518–519

buffered logging, 529

comparison troubleshooting method, 522

console logging, 529

data link layer, 534–537

defining problems, 514

divide-and-conquer troubleshooting method, 520–521

documentation, 502–512, 572

educated guess troubleshooting method, 522

eliminating probable cause, 514

flowcharts, 512–513

follow-the-path troubleshooting method, 521–522

gathering information, 514, 516–517

general troubleshooting procedures, 512–513

hardware troubleshooting tools, 525–528

IP connectivity, 574–576

layered models, 517–518

network layer, 537–539

physical layer, 531–534

process of, 512–523

proposing hypotheses, 514

protocol analyzers, 525

questioning end users, 515–516

- selecting troubleshooting method*, 523
- seven-step troubleshooting process*, 513–515
- SNMP traps*, 530
- software troubleshooting tools*, 524
- solving problems*, 515
- structured troubleshooting methods*, 518–522
- substitution troubleshooting method*, 522
- symptoms/causes of network problems*, 531–545, 573–574
- terminal lines*, 529
- testing hypotheses*, 515
- top-down troubleshooting method*, 519–520
- noise, 534
- output errors, 551
- output queue drops, 550
- performance, 532, 535
- physical layer, verifying, 549–551
- portable network analyzers, 528
- power supplies, 533
- Prime NAM, 528
- process of, 572–573
- protocol analyzers, 525
- routing tables, 539
- SNMP, 543
- software troubleshooting tools, 524
 - baselining tools*, 524
 - knowledge bases*, 524
 - NMS tools*, 524
 - protocol analyzers*, 525
- source ports, 541
- STP failures/loops, 537
- Syslog server, 529–531
- tools, 573
- topology databases, 539
- traffic flows, 541
- transport layer
 - ACL*, 539–542
 - NAT for IPv4*, 542–543
- tunneling protocols, 543
- VPN protocols, 542
- wildcard masks, 541
- trust boundaries, QoS traffic marking**, 378–379
- trust exploitation attacks**, 111
- tunneling**
 - DNS tunneling, 132–133
 - protocols, troubleshooting, 543

- two-tier network design, 461, 464
- Two-Way state, 18–20
- Type of Service field (IPv4), 375

U

- UCS Manager, 593–594
- UDP (User Datagram Protocol), 122, 127, 158
 - flood attacks, 127
 - headers, 126
- unencrypted devices, data loss, 98
- URI (Universal Resource Identifiers), 635, 636
- URL (Uniform Resource Locators), 635
 - blacklisting, 142
 - filtering, 142
- URN (Uniform Resource Names), 635
- USB (Universal Serial Buses)
 - backing up configurations from, 436
 - drives
 - copying router configurations to*, 431–432
 - displaying contents of*, 430
 - verifying connections*, 430–431
 - routers and USB ports, 430

V

- variable delays, 355
- vectors of
 - data loss, 97–98
 - network attacks, 96–97
- verifying
 - ACL, 568–570
 - CDP, 391–393
 - dead intervals, single-area OSPF, 70–71
 - default gateways, 558–560
 - IPv4*, 559
 - IPv6*, 560–562
 - default route propagation, single-area OSPF, 75–77
 - DNS, 570–571
 - dynamic NAT, 249–251
 - extended ACL, 216–218
 - extended ACL edits, 213–214
 - hello intervals, single-area OSPF, 70–71
 - IOS image size in Flash, 439, 440–441
 - LLDP, 397
 - local network addressing, 553–556
 - network paths, 562–566

- NTP, 403–404, 405
- OSPF network type, 46–48
- PAT, 256–257
- physical layer, 549–551
- router configurations to USB drives, 432
- router ID, 38–39
- single-area OSPF, 86–87
 - interface settings*, 81–82
 - neighbors*, 77–79
 - process information*, 80–81
 - protocol settings*, 79–80
- transport layer, 566–567
- video traffic**, 357–360
- virtual circuits**, 275–276, 295–296
- virtual machines (VM), VLAN**, 594
- virtual networks**, 610
 - complexity of, 594–595
 - hypervisors, 592–593
 - switches, 479
 - UCS Manager, 593–594
 - VRF, 595
- virtualization**, 583, 609
 - abstraction layers, 589–590
 - advantages of, 589
 - AWA Management Console, 586
 - cloud computing, 583, 585–586, 609
 - cloud services*, 584
 - community clouds*, 585
 - data centers versus*, 585
 - hybrid clouds*, 584–585
 - IaaS*, 584
 - PaaS*, 584
 - private clouds*, 584
 - public clouds*, 584
 - SaaS*, 584
 - disaster recovery, 589
 - hypervisors, 588, 591–593
 - legacy support, 589
 - prototyping, 589
 - SDN, 592–593, 598, 600, 610–611
 - ACI*, 598, 602–603
 - CEF*, 596
 - central controller*, 597
 - control plane*, 595
 - controller-based SDN*, 605, 611–612
 - controllers*, 600–602
 - data plane*, 596
 - device-based SDN*, 604–605
 - framework*, 599
 - Layer 3 switches*, 596
 - management plane*, 598
 - OpenFlow*, 598
 - OpenStack*, 598
 - policy-based SDN*, 605
 - traditional architectures and*, 599
- servers, 589
 - dedicated servers*, 586–587
 - examples of*, 587–588
- virtual network infrastructure, 592–593
 - complexity of*, 594–595, 610
 - UCS Manager*, 593–594
- VRF, 595
- viruses**, 106–107
- VLAN (Virtual Local Area Networks)**, 556–558, 594
- VM (Virtual Machines), VLAN**, 594
- VNI (Visual Networking Index)**, 357
- voice traffic**, 357–358
- voiceband modems**, 288
- VoIP (Voice over Internet Protocol)**, 294
- VPLS**. *See* Metro Ethernet WAN connectivity
- VPN (Virtual Private Networks)**, 283, 308, 321, 344.
 - See also* IPsec
 - AnyConnect Secure Mobility Client, 321
 - ASA, 321
 - authentication, 339–340
 - PSK*, 339–340
 - RSA*, 340–342
 - benefits of, 322–323
 - client-based VPN, 321, 326
 - clientless VPN, 326
 - cost metrics, 322
 - data integrity, 338–339
 - digital certificates, 327, 333, 335, 339, 341–342, 344–345
 - DMVPN, 330–331
 - enterprise VPN, 324–325
 - GRE over IPsec, 328–329
 - MPLS VPN, 331–332
 - Layer 2 MPLS VPN*, 324, 332–344
 - Layer 3 MPLS VPN*, 324, 332–334
 - PKI, 327, 344
 - protocols, troubleshooting, 542

- remote access VPN, 283, 308, 312, 314–315, 324, 325–326
- scalability, 323
- service provider VPN, 324–325
- site-to-site VPN, 283, 308, 312, 314–315, 323–324, 327–328
- SOHO, 321
- SSL VPN, 326–327
- VTI, 331–332
- VRF (Virtual Routing and Forwarding), 595**
- VTI (Virtual Tunnel Interfaces), 331–332**
- VTY port security, standard IPv4 ACL, 200–203, 220**
- vulnerabilities (security)**
 - defined, 96
 - exploitation tools, 104
 - fuzzers, 103
 - scanners, 104
 - vulnerability brokers, 100

W

WAN (Wide-Area Networks)

- AP, 288
- backbone networks, 287
- backhaul networks, 287
- branch networks, 281
- cable modems, 288
- campus networks, 280
- carrier WAN connections, 278
 - dual-carrier WAN connections, 278–279*
 - single-carrier WAN connections, 278*
- CO, 286
- communications
 - ATM, 296, 324*
 - circuit-switched network communications, 290*
 - demodulation, 288, 295*
 - DWDM multiplexing, 292*
 - Frame Relay networks, 295–296*
 - jitter, 291, 294, 355*
 - latency, 291, 294, 302, 314*
 - modulation, 288, 295*
 - packet-switched network communications, 290–291, 295–296*
 - parallel network communications, 289*
 - SDH cabling standard, 291–292*
 - serial network communications, 289*
 - SONET cabling standard, 291–292*
- connectivity
 - 3G/4G/5G, 302, 307, 314*
 - cable Internet connectivity, 305, 306*
 - circuit-switched WAN connectivity, 295*
 - dedicated broadband WAN connectivity, 297–298*
 - DSL Internet connectivity, 302–304*
 - Internet-based broadband WAN connectivity, 298, 301–311, 314–315*
 - ISDN, 295*
 - ISP Internet connectivity, 309–310*
 - leased-line WAN connectivity, 293–294*
 - LTE, 307*
 - Metro Ethernet WAN connectivity, 298–300, 332*
 - modern WAN connectivity, 296–301, 314*
 - MPLS, 298, 300–301, 324, 332*
 - packet-switched WAN connectivity, 298*
 - PSTN, 295*
 - solution comparisons, 311*
 - teleworking, 283, 302, 308, 312, 314*
 - traditional WAN connectivity, 292–296, 312–313*
 - wired Internet connectivity, 301–302*
 - wireless Internet connectivity, 302*
 - wireless Internet-based broadband connectivity, 306–307*
- core devices, 288
- CPE, 286
- CSU, 288
- DCE, 286–288
- demarcation points, 286
- devices, 287–289
- distributed networks, 282
- DSL modems, 288
- DSU, 288
- DTE, 286–288
- E-carriers, 294
- evolution of, 279–282
- LAN comparisons, 272–273
- local loops (last mile), 286
- operation of, 283–292, 312–313
- optical converters, 288
- OSI model, 284–285
- POP, 286
- private WAN, 273

- public WAN, 273
 - purpose of, 272–282, 312
 - small networks, 279–280
 - standards, 283
 - T-carriers, 294
 - terminology, 285–287
 - toll networks, 286
 - topologies, 274
 - dual-homed WAN topology*, 276
 - fully meshed WAN topology*, 276
 - hub-and-spoke WAN topology*, 275, 330–331
 - partially meshed WAN topology*, 277
 - point-to-point WAN topology*, 274–275
 - voiceband modems, 288
 - wireless routers, 288
 - WAP (Wireless Access Points), PoE**, 485
 - web service API**, 632–633
 - JSON-RPC, 632–633
 - REST, 632–633, 651–652
 - RESTful API, 633–639
 - SOAP, 632
 - XML-RPC, 632–633
 - WFQ (Weight Fair Queuing)**, 362–364
 - white hat hackers**, 99
 - Wi-Fi (802.11), QoS traffic marking**, 373
 - wildcard masks**, 168, 182–183
 - calculating, 170–172
 - examples of, 168–169
 - IPv4
 - address ranges*, 170
 - subnets*, 169–170
 - keywords, 172–173
 - matching hosts, 169–170
 - point-to-point OSPF networks, 40–43
 - troubleshooting, 541
 - WiMAX (Worldwide Interoperability Microwave Access)**, 307
 - wire speeds**, 483
 - wired Internet connectivity**, 301–302
 - wireless connectivity, scalable networks**, 466–467
 - wireless hacking tools**, 103
 - wireless Internet connectivity**, 302
 - wireless Internet-based broadband connectivity**, 306
 - cellular Internet connectivity, 306–307
 - municipal Wi-Fi Internet connectivity, 306
 - satellite Internet connectivity, 307
 - VPN, 283, 308, 321, 344
 - AnyConnect Secure Mobility Client*, 321
 - ASA, 321
 - authentication*, 339–342
 - benefits of*, 322–323
 - client-based VPN*, 321, 326
 - clientless VPN*, 326
 - cost metrics*, 322
 - data integrity*, 338–339
 - digital certificates*, 327, 333, 335, 339, 341–342, 344–345
 - DMVPN, 330–331
 - enterprise VPN*, 324–325
 - GRE over IPsec*, 328–329
 - MPLS VPN, 332
 - PKI, 327, 344
 - remote access VPN*, 283, 308, 312, 314–315, 324–326
 - scalability*, 323
 - service provider VPN*, 324–325
 - site-to-site VPN*, 283, 308, 312, 314–315, 323, 327–328
 - SOHO, 321
 - SSL VPN, 326–327
 - VTI, 331–332
 - VPN. *See also* IPsec
 - WiMAX, 307
 - wireless routers**, 288
 - worms**, 106, 108
 - WRED (Weighted Random Early Detection)**, 371
 - WSA (Web Security Appliance)**, 142–143
-
- ## X
-
- XML (Extensible Markup Language)**, 623, 627–628
 - XML-RPC (Extensible Markup Language-Remote Procedure Call)**, 632–633
-
- ## Y
-
- YAML (YAML Ain't Markup Language)**, 623, 626–627
-
- ## Z
-
- zombies**, 116