

**Save 10%
on Exam
Voucher**

See Inside

PEARSON IT
CERTIFICATION



Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Network+

N10-009



ANTHONY SEQUEIRA
CCIE® No.15626

FREE SAMPLE CHAPTER



Practice
Tests



Flash
Cards



Review
Exercises



Study
Planner

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

- 1.** Go to www.pearsonITcertification.com/register by December 31, 2027.
- 2.** Enter the **print book ISBN:** 9780135367889.
- 3.** Answer the security question to validate your purchase.
- 4.** Go to your account page.
- 5.** Click on the **Registered Products** tab.
- 6.** Under the book listing, click on the **Access Bonus Content** link.

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

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

This page intentionally left blank

CompTIA® Network+

N10-009 Cert Guide

Anthony Sequeira, CCIE No. 15626



CompTIA® Network+ N10-009 Cert Guide

Copyright © 2025 by Pearson Education, Inc.

Hoboken, New Jersey

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

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

ISBN-13: 978-0-13-536788-9

ISBN-10: 0-13-536788-3

Library of Congress Cataloging-in-Publication Data is on file.

\$PrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

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

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

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

**GM K12, Early Career
and Professional
Learning**
Soo Kang

**Director, ITP Product
Management**
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Indexer
Timothy Wright

Proofreader
Donna E. Mulder

Technical Editor
Chris Crayton

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Contents at a Glance

Introduction xxxv

Part I: Networking Concepts

- CHAPTER 1** The OSI Model and Encapsulation 3
- CHAPTER 2** Networking Appliances, Applications, and Functions 35
- CHAPTER 3** Cloud Concepts 65
- CHAPTER 4** Networking Ports, Protocols, Services, and Traffic Types 81
- CHAPTER 5** Transmission Media and Transceivers 101
- CHAPTER 6** Network Topologies, Architectures, and Types 135
- CHAPTER 7** IPv4 Addressing 163
- CHAPTER 8** Evolving Use Cases 203

Part II: Network Implementation

- CHAPTER 9** Routing Technologies 229
- CHAPTER 10** Ethernet Switching Technologies 257
- CHAPTER 11** Configure Wireless Devices and Technologies 285
- CHAPTER 12** Physical Installations 311

Part III: Network Operations

- CHAPTER 13** Organizational Processes and Procedures 325
- CHAPTER 14** Network Monitoring 341
- CHAPTER 15** Disaster Recovery 363
- CHAPTER 16** IPv4 and IPv6 Network Services 385
- CHAPTER 17** Network Access and Management Methods 405

Part IV: Network Security

- CHAPTER 18** Network Security Concepts 425
- CHAPTER 19** Types of Network Attacks 457
- CHAPTER 20** Network Security Features 475

Part V: Network Troubleshooting

- CHAPTER 21** A Network Troubleshooting Methodology 489
CHAPTER 22 Troubleshoot Common Cabling Problems 501
CHAPTER 23 Troubleshoot Common Issues with Network Services 517
CHAPTER 24 Troubleshoot Common Performance Issues 529
CHAPTER 25 Network Troubleshooting Tools 543

Part VI: Final Preparation and Exam Updates

- CHAPTER 26** Final Preparation 577
CHAPTER 27 *CompTIA Network+ N10-009 Cert Guide* Exam Updates 585

Part VII: Appendixes

- APPENDIX A** Answers to Review Questions 587
Index 611

Online Elements

- APPENDIX B** Memory Tables
APPENDIX C Memory Tables Answer Key
APPENDIX D Study Planner
Glossary of Key Terms

Table of Contents

Introduction xxxv

Part I: Networking Concepts

Chapter 1 The OSI Model and Encapsulation 3

Foundation Topics 4

The Purpose of Reference Models 4

The OSI Model 6

Layer 1: The Physical Layer 7

Layer 2: The Data Link Layer 11

Media Access Control 12

Logical Link Control 13

Layer 3: The Network Layer 14

Layer 4: The Transport Layer 17

Layer 5: The Session Layer 19

Layer 6: The Presentation Layer 20

Layer 7: The Application Layer 21

The TCP/IP Stack 22

Layers of the TCP/IP Stack 22

Common Application Protocols in the TCP/IP Stack 26

Real-World Case Study 27

Summary 28

Exam Preparation Tasks 28

Review All the Key Topics 28

Define Key Terms 29

Additional Resources 30

Review Questions 30

Chapter 2 Networking Appliances, Applications, and Functions 35

Foundation Topics 36

Physical and Virtual Appliances 36

Routers 36

Switches 36

Firewalls	45
Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)	46
<i>IDS Versus IPS</i>	46
<i>IDS and IPS Device Categories</i>	47
<i>Signature-Based Detection</i>	48
<i>Policy-Based Detection</i>	48
<i>Anomaly-Based Detection</i>	48
Load Balancer	49
Proxy Servers	49
Network-attached Storage (NAS)	51
Storage Area Networks (SANs)	51
Access Points (APs)	52
Controllers	53
Networking Device Summary	53
Applications and Functions	54
Content Delivery Network (CDN)	54
Virtual Private Network (VPN)	55
Quality of Service (QoS)	55
Time to Live (TTL)	57
Real-World Case Study	57
Summary	58
Exam Preparation Tasks	58
Review All the Key Topics	58
Complete Tables and Lists from Memory	59
Define Key Terms	59
Additional Resources	59
Review Questions	60
Chapter 3 Cloud Concepts	65
Foundation Topics	66
Network Functions Virtualization (NFV)	66
Cloud Networking Components	67

Virtual Private Cloud (VPC)	67
Network Security Groups	68
Network Security Lists	69
Cloud Gateways	69
Deployment Models	71
Service Models	72
Key Cloud Concepts	73
Cloud Connectivity Options	73
Multitenancy	74
Elasticity	74
Scalability	75
Real-World Case Study	75
Summary	75
Exam Preparation Tasks	76
Review All the Key Topics	76
Define Key Terms	76
Additional Resources	76
Review Questions	77

Chapter 4 Networking Ports, Protocols, Services, and Traffic Types 81

Foundation Topics	82
Ports and Protocols	82
FTP (File Transfer Protocol)	82
SFTP	82
SSH	82
Telnet	82
SMTP	83
DNS (Domain Name System)	83
DHCP (Dynamic Host Configuration Protocol)	83
TFTP	83
HTTP	83
NTP	83
SNMP	84
LDAP	84

HTTPS	84
SMB	84
Syslog	84
SMTPS	85
LDAPS	85
Structured Query Language (SQL) Server	85
RDP	85
SIP	85
Protocol/Port Summary	85
Internet Protocol (IP) Types	87
Internet Control Message Protocol (ICMP)	87
Transmission Control Protocol (TCP)	88
User Datagram Protocol (UDP)	88
Generic Routing Encapsulation (GRE)	88
Internet Protocol Security (IPsec)	89
Internet Protocol (IP) Types Summary	89
Traffic Types	90
Unicast	90
Broadcast	91
Multicast	91
Anycast	92
Traffic Types Summary	94
Summary	95
Exam Preparation Tasks	95
Review All the Key Topics	95
Complete Tables and Lists from Memory	96
Define Key Terms	96
Additional Resources	96
Review Questions	97
Chapter 5 Transmission Media and Transceivers	101
Foundation Topics	102
Wireless	102
Transmission Methods	105

WLAN Standards (802.11)	106
<i>802.11a</i>	106
<i>802.11b</i>	106
<i>802.11g</i>	106
<i>802.11n (Wi-Fi 4)</i>	106
<i>802.11ac (Wi-Fi 5)</i>	107
<i>802.11ax (Wi-Fi 6)</i>	107
<i>802.11 Standards Summary</i>	108
Cellular	108
Satellite	109
Copper and Fiber Media and Connectors	111
Coaxial Cable	111
Twisted-Pair Cable	113
<i>Shielded Twisted Pair</i>	113
<i>Unshielded Twisted Pair</i>	114
<i>Twisted-Pair Cable Connectors</i>	116
Plenum Versus Non-plenum Cable	117
Fiber-Optic Cable	117
<i>Multimode Fiber</i>	118
<i>Single-Mode Fiber</i>	120
<i>Fiber-Optic Cable Connectors</i>	120
<i>Fiber Connector Polishing Styles</i>	121
Ethernet and Fiber Standards (802.3)	122
Distance and Speed Limitations	124
Transceivers	126
Multiplexing in Fiber-Optic Networks	127
Media Converters	127
Real-World Case Study	128
Summary	128
Exam Preparation Tasks	128
Review All the Key Topics	128
Complete Tables and Lists from Memory	129
Define Key Terms	129

Additional Resources	130
Review Questions	130
Chapter 6 Network Topologies, Architectures, and Types 135	
Foundation Topics	136
Defining a Network	136
The Purpose of Networks	136
Network Types and Characteristics	137
LAN	137
WAN	138
WLAN	138
SAN	139
Other Categories of Networks	139
CAN	139
MAN	139
PAN	139
Networks Defined Based on Resource Location	140
Client/Server Networks	140
Peer-to-Peer Networks	141
Cloud Networking	143
Networks Defined by Topology	143
Physical Versus Logical Topology	143
Point-to-Point Topology	145
Star Topology	145
Hub-and-Spoke Topology	146
Full-Mesh Topology	147
Partial-Mesh Topology	148
The Three-Tier Hierarchical Model	150
The Access/Edge Layer	150
The Distribution/Aggregation Layer	151
The Core Layer	152
Spine and Leaf	153
Traffic Flows	155

Real-World Case Study	155
Summary	155
Exam Preparation Tasks	156
Review All the Key Topics	156
Complete Tables and Lists from Memory	156
Define Key Terms	157
Additional Resources	157
Review Questions	157
Chapter 7 IPv4 Addressing	163
Foundation Topics	164
Binary Numbering	164
Principles of Binary Numbering	164
Converting a Binary Number to a Decimal Number	165
Converting a Decimal Number to a Binary Number	165
Binary Numbering Practice	167
<i>Binary Conversion Exercise 1</i>	167
<i>Binary Conversion Exercise 1: Solution</i>	168
<i>Binary Conversion Exercise 2</i>	168
<i>Binary Conversion Exercise 2: Solution</i>	168
<i>Binary Conversion Exercise 3</i>	168
<i>Binary Conversion Exercise 3: Solution</i>	169
<i>Binary Conversion Exercise 4</i>	169
<i>Binary Conversion Exercise 4: Solution</i>	170
IPv4 Addressing	170
IPv4 Address Structure	171
Classes of Addresses	173
Assigning IPv4 Addresses	175
IP Addressing Components	175
Static Configuration	176
Dynamic Configuration	180
Automatic Private IP Addressing	180
Subnetting	181

Purpose of Subnetting	182
Subnet Mask Notation	182
Subnet Notation: Practice Exercise 1	184
Subnet Notation: Practice Exercise 1 Solution	184
Subnet Notation: Practice Exercise 2	184
Subnet Notation: Practice Exercise 2 Solution	185
Extending a Classful Mask	185
Borrowed Bits	185
Calculating the Number of Created Subnets	185
Calculating the Number of Available Hosts	186
Basic Subnetting Practice: Exercise 1	187
Basic Subnetting Practice: Exercise 1 Solution	187
Basic Subnetting Practice: Exercise 2	188
Basic Subnetting Practice: Exercise 2 Solution	188
Calculating New IP Address Ranges	189
Advanced Subnetting Practice: Exercise 1	192
Advanced Subnetting Practice: Exercise 1 Solution	192
Advanced Subnetting Practice: Exercise 2	193
Advanced Subnetting Practice: Exercise 2 Solution	193
Additional Practice	195
Classless Inter-domain Routing	196
Real-World Case Study	197
Summary	198
Review All the Key Topics	198
Complete Tables and Lists from Memory	199
Define Key Terms	199
Additional Resources	199
Review Questions	199
Chapter 8 Evolving Use Cases	203
Foundation Topics	205
SDN and SD-WAN	205
Software-Defined Networking (SDN)	205

Software-Defined Wide Area Network (SD-WAN)	206
Virtual Extensible Local Area Network (VXLAN)	208
Zero Trust Architecture (ZTA)	209
SASE and SSE	211
Infrastructure as Code (IaC)	212
IP Version 6	215
Need for IPv6	216
IPv6 Address Structure	217
IPv6 Address Types	217
IPv6 Data Flows	218
<i>Unicast</i>	219
<i>Multicast</i>	219
<i>Anycast</i>	220
Real-World Case Study	221
Summary	222
Exam Preparation Tasks	223
Review All the Key Topics	223
Define Key Terms	223
Additional Resources	224
Review Questions	224

Part II: Network Implementation

Chapter 9 Routing Technologies 229

Foundation Topics	230
Routing	230
Sources of Routing Information	233
Directly Connected Routes	233
Static Routes	234
Dynamic Routing Protocols	235
Routing Protocol Characteristics	237
Believability of a Route	237
Metrics	238
Interior Versus Exterior Gateway Protocols	238
Route Advertisement Method	238
Distance Vector	239

Link State	242
Routing Protocol Examples	242
Address Translation	244
NAT	244
PAT	246
First Hop Redundancy Protocol (FHRP)	248
Real-World Case Study	250
Summary	250
Exam Preparation Tasks	251
Review All the Key Topics	251
Complete Tables and Lists from Memory	252
Define Key Terms	252
Additional Resources	252
Review Questions	253
Chapter 10 Ethernet Switching Technologies	257
Foundation Topics	258
Principles of Ethernet	258
Carrier-Sense Multiple Access with Collision Detection	258
Distance and Speed Limitations	262
Ethernet Switch Features	263
Virtual LANs	263
Switch Configuration for an Access Port	266
Trunks	267
Switch Configuration for a Trunk Port	268
Spanning Tree Protocol	269
Corruption of a Switch's MAC Address Table	269
Broadcast Storms	270
STP Operation	271
Modern Enhancements to STP	274
Link Aggregation	275
LACP Configuration	276
Power over Ethernet	277
Other Switch Features	278

Real-World Case Study	279
Summary	279
Exam Preparation Tasks	280
Review All the Key Topics	280
Complete Tables and Lists from Memory	280
Define Key Terms	280
Additional Resources	281
Review Questions	281
Chapter 11 Configure Wireless Devices and Technologies	285
Foundation Topics	286
Introducing Wireless LANs	286
WLAN Concepts and Components	286
Wireless Routers	286
Wireless Access Point	287
Guest Networks	289
Antennas	289
Channel and Frequency Options	292
Deploying Wireless LANs	293
Types of WLANs	293
IBSS	293
BSS	294
ESS	295
<i>Mesh Topology</i>	295
Sources of Interference	296
Wireless AP Placement	297
Securing Wireless LANs	299
Security Issues	299
Approaches to WLAN Security	300
Security Standards	303
WPA2	303
WPA3	303
Additional Wireless Options	303
Real-World Case Study	304
Summary	305

Exam Preparation Tasks	305
Review All the Key Topics	305
Define Key Terms	306
Additional Resources	306
Review Questions	306

Chapter 12 Physical Installations 311

Foundation Topics	312
Important Installation Implications	312
Locations	313
Power	315
Environmental Factors	317
Real-World Case Study	318
Summary	320
Exam Preparation Tasks	320
Review All the Key Topics	320
Define Key Terms	320
Additional Resources	321
Review Questions	321

Part III: Network Operations

Chapter 13 Organizational Processes and Procedures 325

Foundation Topics	326
Documentation	326
Processes and Procedures	329
Life-cycle Management	329
Change Management	332
Configuration Management	333
Real-World Case Study	334
Summary	335
Exam Preparation Tasks	336
Review All the Key Topics	336
Define Key Terms	336
Additional Resources	336
Review Questions	337

Chapter 14 Network Monitoring 341

Foundation Topics 342

Network Monitoring Methods 342

SNMP 342

Performance Metrics/Sensors 345

Port Mirroring 348

Port Mirroring Configuration 350

Logging 350

Syslog 351

Other Logs 353

NetFlow 354

API Integration 354

Monitoring Solutions 355

Real-World Case Study 357

Summary 357

Exam Preparation Tasks 358

Review All the Key Topics 358

Complete Tables and Lists from Memory 358

Define Key Terms 358

Additional Resources 359

Review Questions 359

Chapter 15 Disaster Recovery 363

Foundation Topics 364

High Availability 364

High-Availability Measurement 364

DR Metrics 364

Fault-Tolerant Network Design 365

Hardware Redundancy 367

Design Considerations for High-Availability Networks 368

High-Availability Best Practices 369

Content Caching 370

Load Balancing 370

Hardware Redundancy 370

Testing 372

Real-World Case Study: Network Design	372
Case Study Scenario	373
Suggested Solution	375
IP Addressing	375
Layer 1 Media	376
Layer 2 Devices	376
Layer 3 Devices	377
Wireless Design	378
Environmental Factors	379
Cost Savings Versus Performance	379
Topology	379
Summary	380
Exam Preparation Tasks	380
Review All the Key Topics	380
Define Key Terms	381
Additional Resources	381
Review Questions	381
Chapter 16 IPv4 and IPv6 Network Services	385
Foundation Topics	386
Dynamic Addressing	386
DHCP	386
SLAAC	389
Name Resolution	390
DNS	391
Hosts File	396
Time Protocols	397
NTP	397
PTP	398
NTS	399
Real-World Case Study	399
Summary	400
Exam Preparation Tasks	400
Review All the Key Topics	400
Complete Tables and Lists from Memory	401

Define Key Terms 401
Additional Resources 401
Review Questions 401

Chapter 17 Network Access and Management Methods 405

Foundation Topics 406
Virtual Private Networks (VPNs) 406
 IPsec 408
 IKE 408
 Authentication Header and Encapsulating Security Payload 410
 The Five Steps in Setting Up and Tearing Down an IPsec Site-to-Site VPN Using IKEv1 412
 IKEv2 413
 Other VPN Technologies 413
Other Network Access Technologies 414
Authentication and Authorization Considerations 417
In-Band vs. Out-of-Band Management 418
Real-World Case Study 418
Summary 419
Exam Preparation Tasks 419
Review All the Key Topics 419
Complete Tables and Lists from Memory 420
Define Key Terms 420
Additional Resources 420
Review Questions 420

Part IV: Network Security

Chapter 18 Network Security Concepts 425

Foundation Topics 426
Core Security Concepts 426
 Confidentiality, Integrity, and Availability (CIA) 426
 Confidentiality 426
 Symmetric Encryption 427
 Asymmetric Encryption 428
 Integrity 430

<i>Availability</i>	431
Threats, Vulnerabilities, Risks, and Exploits	431
<i>Threats</i>	432
<i>Vulnerabilities</i>	432
<i>Risks</i>	433
<i>Exploits</i>	433
Least Privilege	433
Role-Based Access Control	434
Defense in Depth	434
<i>Screened Subnet</i>	435
<i>Separation of Duties</i>	435
<i>Network Access Control</i>	435
<i>Honeypot</i>	435
Network Segmentation Enforcement	436
<i>IoT and IIoT</i>	436
<i>SCADA, ICS, and OT</i>	437
<i>Guest Networks</i>	437
<i>BYOD</i>	437
Authentication Methods	438
Multifactor	438
TACACS+	439
Single Sign-On	439
RADIUS	439
LDAP	440
Kerberos	440
SAML	441
Time-based Authentication	441
Local Authentication	441
Risk Management and SIEM	441
Risk Management	441
Security Risk Assessments	442
<i>Threat Assessment</i>	442
<i>Vulnerability Assessment</i>	442
<i>Penetration Testing</i>	442

<i>Posture Assessment</i>	442
Business Risk Assessment	442
<i>Process Assessment</i>	443
<i>Vendor Assessment</i>	443
Security Information and Event Management (SIEM)	443
Physical Security	444
Detection Methods	444
Prevention Methods	445
Audits and Regulatory Compliance	447
Real-World Case Study	448
Summary	449
Exam Preparation Tasks	449
Review All the Key Topics	449
Define Key Terms	450
Additional Resources	450
Review Questions	451

Chapter 19 Types of Network Attacks 457

Foundation Topics	458
Technology-Based Attacks	458
Denial-of-Service (DoS)	458
Distributed Denial-of-Service (DDoS)	459
On-Path Attack	459
DNS Poisoning	460
VLAN Hopping	460
ARP Poisoning	460
ARP Spoofing	461
Rogue DHCP	461
Rogue Access Point	461
Evil Twin	461
Ransomware	461
Password Attacks	462
MAC Spoofing	462
MAC Flooding	462

IP Spoofing	463
Deauthentication	463
Malware	463
Social Engineering Attacks	464
Other Miscellaneous Attacks	465
Real-World Case Study	469
Summary	470
Exam Preparation Tasks	470
Review All the Key Topics	470
Define Key Terms	471
Additional Resources	471
Review Questions	471
Chapter 20 Network Security Features	475
Foundation Topics	476
Device Hardening	476
Best Practices	476
Network Access Control (NAC)	480
Other Network Security Features	482
Real-World Case Study	483
Summary	483
Exam Preparation Tasks	484
Review All the Key Topics	484
Define Key Terms	484
Additional Resources	484
Review Questions	485

Part V: Network Troubleshooting

Chapter 21 A Network Troubleshooting Methodology	489
Foundation Topics	490
Troubleshooting Basics	490
Troubleshooting Fundamentals	490
Structured Troubleshooting Methodology	492
Real-World Case Study	495
Summary	495

Exam Preparation Tasks	496
Review All the Key Topics	496
Complete Tables and Lists from Memory	496
Define Key Terms	496
Additional Resource	496
Review Questions	497

Chapter 22 Troubleshoot Common Cabling Problems 501

Foundation Topics	502
Specifications and Limitations	502
Common Cable Issues	502
Common Interface Issues	505
Common Hardware Issues	506
Common Tools	507
Real-World Case Study	511
Summary	512
Exam Preparation Tasks	512
Review All the Key Topics	512
Define Key Terms	512
Additional Resources	513
Review Questions	513

Chapter 23 Troubleshoot Common Issues with Network Services 517

Foundation Topics	518
Considerations for General Network Troubleshooting	518
Common Network Service Issues	519
Real-World Case Study	523
Summary	524
Exam Preparation Tasks	524
Review All the Key Topics	524
Define Key Terms	524
Additional Resources	525
Review Questions	525

Chapter 24 Troubleshoot Common Performance Issues 529

Foundation Topics	530
Network Performance Considerations	530

Wireless Performance Considerations	531
Other Wireless Considerations	533
Antennas	533
Frequencies and Channels	533
More Considerations	534
Common Wireless Issues	534
Wireless Network Troubleshooting	536
Wireless Network Troubleshooting Solution	536
Real-World Case Study	537
Summary	538
Exam Preparation Tasks	538
Review All the Key Topics	538
Define Key Terms	538
Review Questions	539
Chapter 25 Network Troubleshooting Tools	543
Foundation Topics	544
Software Tools	544
Protocol Analyzer/Packet Capture	544
Bandwidth Speed Tester	544
Port Scanner	544
iperf	545
NetFlow Analyzers	546
TFTP Server	546
Terminal Emulator	546
IP Scanner	546
LLDP/CDP	546
Command-Line Tools	547
ping	547
ping with IPv6	549
ipconfig	549
ifconfig	553
ip	554

nslookup	554
dig	556
traceroute	557
traceroute for IPv6	558
arp	558
netstat	560
hostname	562
route	562
telnet	567
tcpdump	567
nmap	567
Basic Networking Device Commands	567
Hardware Tools	568
Wi-Fi Analyzer	568
Tone Generator	569
Cable Tester	569
Tap	569
Visual Fault Locator	569
Real-World Case Study	570
Summary	570
Exam Preparation Tasks	570
Review All the Key Topics	570
Complete Tables and Lists from Memory	571
Define Key Terms	571
Additional Resources	572
Review Questions	572

Part VI: Final Preparation and Exam Updates

Chapter 26 Final Preparation 577

Tools for Final Preparation	577
Video Training	578
Memory Tables	578
End-of-Chapter Review Tools	579

Suggested Plan for Final Review and Study	579
Strategies for Taking the Exam	581
Summary	582
Chapter 27 CompTIA Network+ N10-009 Cert Guide Exam Updates	585
Always Get the Latest at the Book's Product Page	585
Technical Content	586

Part VII: Appendixes

Appendix A Answers to Review Questions	587
Index	611

Online Elements

Appendix B Memory Tables
Appendix C Memory Tables Answer Key
Appendix D Study Planner
Glossary of Key Terms

About the Author

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

Dedication

This book is dedicated to my daughter, Bella Sequeira, who inspires me to do great work every day.

Acknowledgments

I cannot thank Nancy Davis and Chris Cleveland enough for their patience as I created this latest edition of the text. Also, huge thanks to my editors, Chris Crayton and Bill McManus. Their work on this text improved it dramatically.

About the Technical Reviewer

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge. Chris tech edited and contributed to this book to make it better for students and those wishing to better their lives.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *CompTIA Network+ N10-009 Cert Guide* for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonITcertification.com/register and log in or create an account.* Enter the product ISBN 9780135367889 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

Introduction

The CompTIA Network+ certification is a popular certification for those entering the computer networking field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA Network+ certification is unique in that it is vendor neutral. It does not focus its content on the techniques and technologies of any one specific network vendor. The CompTIA Network+ certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by Cisco Systems.

On the CompTIA Network+ exam, the topics are mostly generic in that they can apply to networking equipment regardless of vendor. Although the CompTIA Network+ certification is vendor neutral, network software and systems are implemented by multiple independent vendors. Therefore, several of the exercises, examples, and simulations in this book include using particular vendors' configurations and technologies, such as Microsoft Windows operating systems or Cisco Systems routers and switches. More detailed training for a specific vendor's software and hardware can be found in books and training specific to that vendor.

Who Should Read This Book?

This book was written with two audiences in mind: those who want to learn all they can about networking technology and those who want to pass the CompTIA Network+ exam. I think that both groups are going to be very impressed with the breadth of technologies this book details. Although it would be impossible to cover every topic in networking today, this book manages to cover all the massive areas that make networking an exciting field that many people want to learn.

Readers will range from people who are attempting to attain a position in the IT field to people who want to keep their skills sharp or perhaps retain their job when facing a company policy that mandates they take the new exams. This book is also for those who want to acquire additional certifications beyond the Network+ certification (for example, the Cisco Certified Network Associate [CCNA] certification and beyond). The book is designed to enable an easy transition to future certification studies.

Resources

This book comes with a wealth of digital resources to help you review, practice, and assess your knowledge. The end of each chapter contains a review section that references several of these tools, and you should be sure to use them as you complete each chapter to help reinforce what you are learning. You can use them again after

you finish the book to help review and make sure you are fully prepared for the exam.

Here's a list of resources available on the companion website:

- Interactive glossary flash card application
- Interactive exam essentials appendix
- The Pearson Test Prep (PTP) practice test app
- Video training on key exam topics
- Memory table review exercises and answer keys
- A study planner tool
- Instructions to redeem your Network+ certification exam voucher, which provides a 10% discount on the exam

To access the companion website, follow these steps:

- Step 1.** Go to <https://www.pearsonITcertification.com/register> by December 31, 2027.
- Step 2.** Either log in to your account if you have an existing account already or create a new account.
- Step 3.** Enter the ISBN of this book (**9780135367889**) and click **Submit**.
- Step 4.** Answer the challenge questions to validate your purchase.
- Step 5.** In your account page, click the **Registered Products** tab and then click the **Access Bonus Content** link.

How to Access the Pearson Test Prep (PTP) App

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

- You can get your access code by registering the print ISBN (9780135367889) on [pearsonITcertification.com/register](https://www.pearsonITcertification.com/register). Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.

- Premium Edition: If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at pearsonITcertification.com, click Account to see details of your account, and click the digital purchases tab.

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

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

- Step 1.** Open this book’s companion website as shown earlier on the first page of the book, under the “Companion Website and Pearson Test Prep Access Code” heading.
- Step 2.** Click the **Practice Exams** button.
- Step 3.** Follow the instructions listed there for both installing the desktop app and for using the web app.

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

Customizing Your Exams

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

- **Study mode:** Enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing

multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

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

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

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

Updating Your Exams

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

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

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

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the Network+ N10-009 blueprint from CompTIA. This book also helps you prepare for the N10-009 version of the CompTIA Network+ exam.

To aid you in mastering and understanding the Network+ certification objectives, this book uses the following methods:

- **Opening topics list:** This list spells out the Network+ objectives and topics that are covered in the chapter.
- **Foundation topics:** At the heart of a chapter, the sections under “Foundation Topics” explain the topics from hands-on and theory-based standpoints. These sections include in-depth descriptions, tables, and figures that build your knowledge so that you can pass the N10-009 exam. Each chapter is broken into multiple sections.
- **Key topics:** The “Review All Key Topics” section indicates important figures, tables, and lists of information that you need to review for the exam. Key Topic icons are sprinkled throughout each chapter, and a table at the end of each chapter lists the important parts of the text called out by these icons.
- **Memory tables:** You can find memory tables and their answer key on the book’s companion website in Appendixes B and C, respectively. Use them to help memorize important information.
- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the definitions in the Glossary. On the companion website, you will find a flash card application with all the glossary terms separated by chapter, and you can use it to study key terms as well.
- **Practice exams:** As previously described, this book comes complete with several full-length practice exams available to you in the Pearson Test Prep practice test software, which you can download and install from the companion website. The Pearson Test Prep software is also available to you online, at www.PearsonTestPrep.com. Follow the directions at the beginning of the book under “Companion Website and Pearson Test Prep Access Code.” Be sure to run through the questions in exam bank 1 as you complete each chapter in study mode. When you have completed the book, take a full practice test using exam bank 2 questions in practice exam mode to test your exam readiness.

For current information about the CompTIA Network+ certification exam, visit <https://www.comptia.org/certifications/network>.

Strategies for Exam Preparation

This book comes with a study planner tool on the companion website. It is a spreadsheet that helps you keep track of the activities you need to perform in each chapter and helps you organize your exam preparation tasks. As you read the chapters in this book, jot down notes with key concepts or configurations in the study planner. Each chapter ends with a summary and series of exam preparation tasks to help you reinforce what you have learned. These tasks include review exercises such as reviewing key topics, completing memory tables, defining key terms, answering review questions, and performing exercises. Make sure you perform these tasks as you complete each chapter to improve your retention of the material and record your progress in the study planner.

The book concludes with Chapter 26, “Final Preparation,” which offers you guidance on your final exam preparation and provides you with some helpful exam advice. Make sure you read over that chapter to help assess your exam readiness and identify areas where you need to focus your review.

Download the current exam objectives by submitting a form on the following web page: <https://www.comptia.org/certifications/network>.

Use the practice exams, which are included on this book’s companion website. As you work through the practice exams, use the practice test software reporting features to note the areas where you lack confidence and then review the related concepts. After you review those areas, work through the practice exams a second time and rate your skills. Keep in mind that the more you work through the practice exams, the more familiar the questions become, and the less accurately the practice exams judge your skills.

After you work through the practice exams a second time and feel confident with your skills, schedule the real CompTIA Network+ exam (N10-009).

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (*objectives*) and specific topics under each general topic (*subobjectives*) for the CompTIA Network+ N10-009 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters in the book.

Table I-1 CompTIA Network+ Exam Topics

Chapter	N10-009 Exam Objective	N10-009 Exam Subobjective
Chapter 1: The OSI Model and Encapsulation	1.0 Networking Concepts	1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference model.
Chapter 2: Networking Appliances, Applications, and Functions	1.0 Networking Concepts	1.2 Compare and contrast networking appliances, applications, and functions.
Chapter 3: Cloud Concepts	1.0 Networking Concepts	1.3 Summarize cloud concepts and connectivity options.
Chapter 4: Networking Ports, Protocols, Services, and Traffic Types	1.0 Networking Concepts	1.4 Explain common networking ports, protocols, services, and traffic types.
Chapter 5: Transmission Media and Transceivers	1.0 Networking Concepts	1.5 Compare and contrast transmission media and transceivers.
Chapter 6: Network Topologies, Architectures, and Types	1.0 Networking Concepts	1.6 Compare and contrast network topologies, architectures, and types.
Chapter 7: IPv4 Addressing	1.0 Networking Concepts	1.7 Given a scenario, use appropriate IPv4 network addressing.
Chapter 8: Evolving Use Cases	1.0 Networking Concepts	1.8 Summarize evolving use cases for modern network environments.
Chapter 9: Routing Technologies	2.0 Network Implementation	2.1 Explain characteristics of routing technologies.
Chapter 10: Ethernet Switching Technologies	2.0 Network Implementation	2.2 Given a scenario, configure switching technologies and features.
Chapter 11: Configure Wireless Devices and Technologies	2.0 Network Implementation	2.3 Given a scenario, select and configure wireless devices and technologies.
Chapter 12: Physical Installations	2.0 Network Implementation	2.4 Explain important factors of physical installations.
Chapter 13: Organizational Processes and Procedures	3.0 Network Operations	3.1 Explain the purpose of organizational processes and procedures.
Chapter 14: Network Monitoring	3.0 Network Operations	3.2 Given a scenario, use network monitoring technologies.
Chapter 15: Disaster Recovery	3.0 Network Operations	3.3 Explain disaster recovery (DR) concepts.

Chapter	N10-009 Exam Objective	N10-009 Exam Subobjective
Chapter 16: IPv4 and IPv6 Network Services	3.0 Network Operations	3.4 Given a scenario, implement IPv4 and IPv6 network services.
Chapter 17: Network Access and Management Methods	3.0 Network Operations	3.5 Compare and contrast network access and management methods.
Chapter 18: Network Security Concepts	4.0 Network Security	4.1 Explain the importance of basic network security concepts.
Chapter 19: Types of Network Attacks	4.0 Network Security	4.2 Summarize various types of attacks and their impact to the network.
Chapter 20: Network Security Features	4.0 Network Security	4.3 Given a scenario, apply network security features, defense techniques, and solutions.
Chapter 21: A Network Troubleshooting Methodology	5.0 Network Troubleshooting	5.1 Explain the troubleshooting methodology.
Chapter 22: Troubleshoot Common Cabling Problems	5.0 Network Troubleshooting	5.2 Given a scenario, troubleshoot common cabling and physical interface issues.
Chapter 23: Troubleshoot Common Issues with Network Services	5.0 Network Troubleshooting	5.3 Given a scenario, troubleshoot common issues with network services.
Chapter 24: Troubleshoot Common Performance Issues	5.0 Network Troubleshooting	5.4 Given a scenario, troubleshoot common performance issues.
Chapter 25: Network Troubleshooting Tools	5.0 Network Troubleshooting	5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use:

- **Chapter 1: The OSI Model and Encapsulation**—This chapter details the OSI model and its seven layers. This chapter also presents the encapsulation and deencapsulation processes associated with this important model.
- **Chapter 2: Networking Appliances, Applications, and Functions**—This chapter presents commonly used physical and virtual appliances in use in

networks today. This chapter also covers commonly used applications and network functions.

- **Chapter 3: Cloud Concepts**—This chapter covers some of the most important cloud concepts used in modern networking. Just some of the topics covered include deployment models, service models, and cloud connectivity options.
- **Chapter 4: Networking Ports, Protocols, Services, and Traffic Types**—This chapter ensures you are familiar with some of the most popular ports, protocols, and services in use today. This chapter also covers the traffic types of unicast, multicast, anycast, and broadcast.
- **Chapter 5: Transmission Media and Transceivers**—This chapter is all about the wireless and wired connections we make in modern networks. This chapter also covers the transceivers and connector types we often see in our networks today.
- **Chapter 6: Network Topologies, Architectures, and Types**—This chapter covers common network topologies, including mesh, hybrid, hub and spoke, and more. This chapter also covers common traffic flow types found in today's networking environments.
- **Chapter 7: IPv4 Addressing**—This chapter is all about IPv4 addressing. This includes coverage of public versus private IP addressing, subnetting, and the IPv4 address classes.
- **Chapter 8: Evolving Use Cases**—This chapter is all about some of the more cutting-edge technologies appearing in our most modern of networks today. Just some of the technologies that are covered include software-defined networking, Virtual Extensible Local Area Network (VXLAN), and IPv6 addressing.
- **Chapter 9: Routing Technologies**—This chapter tackles technologies that are specific to routing in our networks. This includes such topics as static versus dynamic routing, route selection, address translation, and first hop redundancy protocols.
- **Chapter 10: Ethernet Switching Technologies**—This chapter describes technologies related to switching in today's networks. This includes such topics as VLANs, switch interface configurations, and Spanning Tree Protocol.
- **Chapter 11: Configure Wireless Devices and Technologies**—This chapter examines topics related to Wi-Fi in networks today. This includes topics such as frequency options, network types, encryption, and many more.

- **Chapter 12: Physical Installations**—This chapter examines several important factors you should consider when you are planning and operating physical installations for networking equipment. This chapter includes topics like power and environmental factors.
- **Chapter 13: Organizational Processes and Procedures**—This chapter focuses on the purpose of organizational processes and procedures. Topics like documentation, life-cycle management, change management, and configuration management are all covered.
- **Chapter 14: Network Monitoring**—This chapter presents many different options and methods when it comes to monitoring modern networks. Topics include SNMP, SIEMs, and many more.
- **Chapter 15: Disaster Recovery**—This chapter focuses on disaster recovery (DR) topics. This includes things like DR metrics, DR sites, and high-availability approaches.
- **Chapter 16: IPv4 and IPv6 Network Services**—This chapter presents many examples of popular IPv4 and IPv6 services found in networks today. Topics in this chapter include dynamic addressing options, name resolution services, and time protocols.
- **Chapter 17: Network Access and Management Methods**—This chapter presents various options available today for network access and network management. Topics include VPNs, connection methods, and specific technologies like jump boxes.
- **Chapter 18: Network Security Concepts**—This chapter is a big one. Why? It tackles the hugely important topic of basic network security concepts. Here you will learn about things like logical security, physical security, and common security terminology.
- **Chapter 19: Types of Network Attacks**—What are some of the most common network attacks in use today? This chapter addresses this question head on and covers such topics as DoS and DDoS attacks, social engineering attacks, and many, many more.
- **Chapter 20: Network Security Features**—This chapter covers network security features, defense techniques, and solutions. This includes a discussion of device hardening, network access controls, key management, security rules, and zones.
- **Chapter 21: A Network Troubleshooting Methodology**—This chapter provides guidance on a well-planned and effective troubleshooting methodology. This methodology begins with problem identification and ends with the documentation of findings.

- **Chapter 22: Troubleshoot Common Cabling Problems**—This chapter covers troubleshooting common cabling and physical interface issues. The chapter focuses on three main areas: cable issues, interface issues, and hardware issues.
- **Chapter 23: Troubleshoot Common Issues with Network Services**—This chapter focuses on troubleshooting common issues with network services. This includes the two main areas of switching- and routing-based services.
- **Chapter 24: Troubleshoot Common Performance Issues**—These days, a network that is performing poorly can be nearly as disruptive as a network that is not functioning at all. This chapter guides you through troubleshooting the most common of performance issues. Both wired and wireless networks are discussed.
- **Chapter 25: Network Troubleshooting Tools**—This chapter focuses on the use of network troubleshooting tools that can help you solve common issues. This includes the three main categories of tools: software tools, hardware tools, and basic networking device commands.

Figure Credits

Figures 3-1 to 3-3 © 2024, Amazon Web Services, Inc.

Figures 13-3 and 20-1 © 2024, Linksys Holdings, Inc.

Figures 7-4 to 7-12, 13-2 and 16-2 © 2024, Microsoft

Figures 7-14 and 14-7 © 2024 SolarWinds Worldwide, LLC

Figures 14-3 and 25-1 © Wireshark Foundation

Figure 22-2, photo courtesy of Digi.Key Corporation (<http://www.digikey.com>)

Figure 22-3, photo courtesy of Coral.i Solutions (<http://www.coral.i.com>)

Cover image, Funtap/shutterstock

Figures 2-2 to 2-18, 4-1 to 4-4, 5-2, 6-1 to 6-10, 7-13, 8-1, 8-3 to 8-5, 9-1 to 9-16, 10-1, 10-4 to 10-8, 10-10 to 10-17, 11-1 to 11-7, 11-11, 14-1, 14-2, 14-4 to 14-6, 15-1 to 15-4, 15-6, 16-1, 16-3, 17-1, 17-2, 17-4, 18-1, 18-2, 19-1, 24-1 courtesy of Cisco Systems, Inc.

Evolving Use Cases

Are you excited to learn about some of the newer technologies featured in this version of the CompTIA Network+ exam? As the title of this chapter suggests, here we are going to focus on some of the latest evolving technologies taking the networking world by storm (and no, not a broadcast storm).

This chapter begins with a look at software-defined networking (SDN) and a very specific implementation called the software-defined wide area network (SD-WAN). As you will learn, these technologies make it much simpler to operate modern networks with all their sophisticated capabilities and features.

Next, this chapter explores the latest evolution in virtual local area networks. It is called virtual extensible local area network, or VXLAN. As you will learn, VXLAN is a network virtualization technology that encapsulates Ethernet frames in UDP packets to create a scalable Layer 2 overlay network across Layer 3 infrastructures. It enables the extension of VLANs beyond traditional boundaries, supporting large-scale cloud and data center environments by allowing for more flexible and dynamic network segmentation.

As one would guess, another important area of evolving technologies for networking is in the space of security. In this part of the chapter, we examine some of the latest advancements in network security. These include zero trust architecture (ZTA), Secure Access Secure Edge (SASE), and Security Service Edge (SSE).

Next, this chapter describes many aspects and benefits of infrastructure as code (IaC). Infrastructure as code is a method of managing and provisioning computing infrastructure through machine-readable configuration files, enabling automation and consistency across environments. Treating infrastructure configurations as code allows for version control, collaborative development, and efficient scaling of IT resources.

Although IPv4 is the most widely deployed Layer 3 addressing scheme in today's networks, its scalability limitations are causing available IPv4 addresses to quickly become depleted. Fortunately, a newer version of IP, IPv6, is scalable beyond anything you will need in your lifetime. This chapter concludes by introducing you to the fundamental characteristics of IPv6 addressing.

Foundation Topics

SDN and SD-WAN

Never before in my decades of studying and teaching computer networking have I seen more fear from students regarding the elimination of their jobs due to automation and cutting-edge technologies. In this author's opinion, artificial intelligence (AI) and computers are not going to be eliminating the need for you (a human) in the network any time soon. While *software-defined networking (SDN)* allows you to add more and more automation and orchestration to a network, there will still be a need for you and your skills.



Software-Defined Networking (SDN)

Software-defined networking, which has been around for a very long time, is making a huge resurgence and being implemented in many parts of large and small networks today. For example, consider your wireless LAN. Perhaps you are using lightweight access points and wireless LAN controllers (WLCs). If so, you are seeing a very strict separation of the data, management, and control planes. The WLC is the primary control plane intelligence of the solution. (The specific SDN planes of operation are covered in more detail later in this chapter.)

SDN is changing the landscape of traditional networks. A well-implemented software-defined network allows the administrator to implement features, functions, and configurations without the need to do command-line configuration on the individual network devices. The front end that the administrator interfaces with can alert the administrator to what the network is currently doing, and then, through that same graphical user interface, the administrator can indicate what he or she wants done; behind the scenes, the software-defined network implements the detailed configurations across multiple network devices.

A key component in most software-defined networking solutions is an SDN controller. This appliance-based device is responsible for distributing control plane instructions to network devices downstream for configuration and management.

While many different approaches can be taken to SDN, almost everyone agrees that the best strategy is to separate the network into different discrete planes or layers of operation:

- **Application plane:** This is where all the technology that involves the applications resides. Today, it is not uncommon for an application to be powered by tiny microservices running as containers in a heavily virtualized cloud

environment. But of course, there are plenty of other options for powering this layer. Many of them can even be much more traditional.

- **Control plane:** Although this layer of operation is often described as the “brains” of the operation, you are still the true brains of the operation. In fact, you are likely to use a “single pane of glass” solution that provides the correct application programming interface (API) calls to the controller. The controller turns these API commands into calls to the network devices in order to monitor or configure them properly. The API calls from you to the controller are referred to as *northbound operations*, and the commands from the controller to the network devices are referred to as *southbound operations*. The controller is always considered to be in the middle. Examples of control layer functions include routing and switching intelligence, and common control layer protocols include Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Rapid Spanning Tree Protocol (RSTP).
- **Data plane:** The data plane (sometimes called the infrastructure plane) contains the hardware and software that power the enterprise. In it, you often find legacy and dated technologies. This infrastructure is now being controlled in a new and exciting way.
- **Management plane:** It is necessary to perform a lot of routine maintenance in a network, and the management plane is for these “boring” tasks. The management plane allows administrators to see their devices and traffic flows and react as needed to manage data plane behavior. This can be done automatically through configuration apps that can, for example, add more bandwidth if it looks as if edge components are getting congested. Note that the management plane manages and monitors processes across all layers of the network stack.

All the layers of operation are critically important, and each plays an important role. The layers of operation work seamlessly together as one to get the various jobs done. Figure 8-1 shows these commonly defined planes of operations with software-defined networking.

Software-Defined Wide Area Network (SD-WAN)

For many years, new technologies and improvements have been made in local area networks (LANs). Sadly, there were not many innovations in a very important part of the network—the wide area network (WAN). Thanks to software-defined networking improvements, we now have a celebrated and popular new improvement called the *software-defined wide area network (SD-WAN)*.

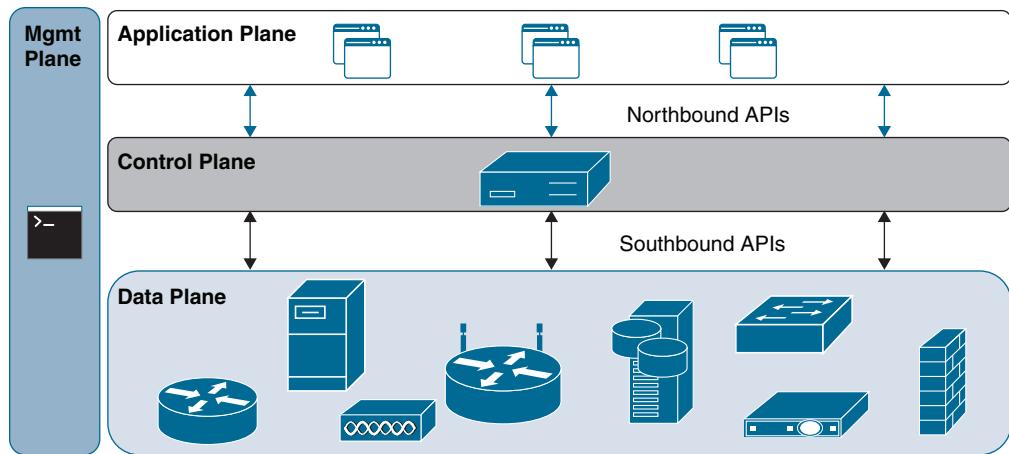


Figure 8-1 Software-Defined Networking

The SD-WAN is a transformative approach to managing and optimizing wide area networks. Unlike traditional WANs, which rely on proprietary hardware and inflexible connectivity options, SD-WAN utilizes software-defined networking principles to create a more adaptable and efficient network infrastructure. SD-WAN abstracts the network layer from the hardware, enabling centralized control and dynamic management of network traffic across multiple connection types, such as broadband, Multiprotocol Label Switching (MPLS), Long-Term Evolution (LTE), and more. This abstraction enhances performance, reduces costs, and improves overall agility, making it particularly valuable for enterprises with distributed branch locations.

One of the key features of SD-WAN is its ***application awareness***. This capability allows the network to identify and prioritize traffic based on the application, ensuring that critical applications, such as video conferencing and VoIP, receive the necessary bandwidth and low latency for optimal performance. Application awareness in SD-WAN is achieved through deep packet inspection and real-time analytics, which categorize and manage traffic flows according to predefined policies. This feature not only improves the quality of experience for end users but also enhances overall network efficiency by intelligently routing traffic based on application requirements and current network conditions.

Zero-touch provisioning (ZTP) is another significant feature of SD-WAN, simplifying the deployment and management of network devices. With ZTP, network administrators can configure and deploy new branch devices without manual intervention. This process typically involves shipping a preconfigured device to a location, where it automatically connects to the SD-WAN controller, downloads its configuration, and becomes operational with minimal human involvement. ZTP

significantly reduces deployment time and operational costs, enabling rapid scaling of the network to meet the needs of growing businesses and facilitating easier maintenance and updates.

SD-WAN is designed to be *transport agnostic*, meaning it can leverage any available connectivity option, such as broadband, MPLS, LTE, or even satellite links. This flexibility allows organizations to choose the most cost-effective and efficient connectivity for each location, without being tied to a specific provider or technology. Transport agnosticism enhances the resilience and redundancy of the network, as SD-WAN can dynamically route traffic across multiple links to maintain performance and availability, even in the event of a link failure or degradation.

Central policy management is a cornerstone of SD-WAN architecture, providing a unified platform for defining and enforcing network policies across all connected devices and locations. Through a centralized management console, administrators can easily set rules for traffic prioritization, security, and compliance, ensuring consistent policy application throughout the network. This centralized approach simplifies network management, improves security by standardizing configurations, and enables quick adjustments to network policies in response to changing business needs or threats. Central policy management also allows for real-time monitoring and analytics, providing valuable insights into network performance and usage.

Key Topic

Virtual Extensible Local Area Network (VXLAN)

Virtual Extensible Local Area Network (VXLAN) is a network virtualization technology designed to address the limitations of traditional VLANs in large-scale data center environments and the cloud. It operates by encapsulating Layer 2 Ethernet frames within Layer 3 UDP packets, enabling the extension of Layer 2 networks over a Layer 3 infrastructure. This encapsulation allows for the creation of large-scale, logical Layer 2 networks across geographically dispersed data centers, which facilitates the movement of virtual machines (VMs) and workloads without reconfiguring the underlying physical network.

At its core, VXLAN provides a way to overcome the scalability limitations of traditional VLANs, which are restricted to a maximum of 4096 segments due to the 12-bit VLAN ID field. By using a 24-bit segment identifier known as a VXLAN Network Identifier (VNI), VXLAN can support up to 16 million distinct segments. This significant increase in segmentation capacity is crucial for modern cloud environments and large enterprise data centers, where thousands of tenants and millions of isolated networks might coexist.

The key mechanism that makes VXLAN powerful is its ability to perform *Layer 2 encapsulation*. In VXLAN, a Layer 2 Ethernet frame from a VM or host is encapsulated into a Layer 3 UDP packet. This packet includes an outer IP header, which

can route across a Layer 3 network, and an outer UDP header, which facilitates the tunneling mechanism. The encapsulated packet is then transmitted over the existing Layer 3 infrastructure. This process allows for Layer 2 segments to be extended across different Layer 3 networks, creating a seamless and scalable virtual network that behaves as if all connected hosts are on the same local network. Figure 8-2 shows the Layer 2 encapsulation used with VXLAN technology.

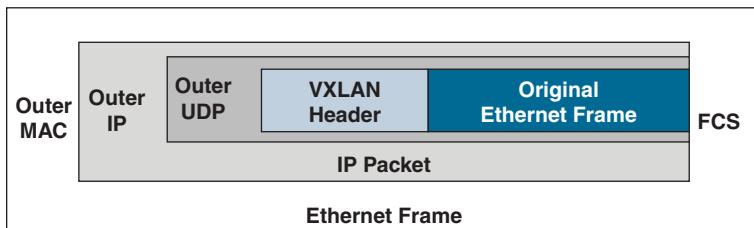


Figure 8-2 VXLAN Encapsulation

One of the primary applications of VXLAN is in ***data center interconnect (DCI)***. DCI involves connecting multiple data centers to provide a unified infrastructure, allowing for efficient resource sharing, workload mobility, and disaster recovery. VXLAN is particularly suited for DCI because it enables the extension of Layer 2 networks over Layer 3 distances, thus facilitating the seamless migration of VMs and applications between data centers. This capability is crucial for businesses that need to maintain high availability and disaster resilience by distributing workloads across multiple locations.

VXLAN also integrates well with modern network management and automation tools, supporting dynamic and programmable networking. The VXLAN gateways or Virtual Tunnel Endpoints (VTEPs) play a critical role in encapsulating and decapsulating traffic and can be implemented in both hardware (switches) and software (hypervisors). This flexibility makes VXLAN an essential component in the architecture of software-defined networks (SDNs) and network functions virtualization (NFV), where it provides the necessary overlay networks that decouple virtual network management from physical network hardware.

Key Topic

Zero Trust Architecture (ZTA)

Zero trust architecture (ZTA) is a security model centered on the principle that no entity, whether inside or outside the network, should be trusted by default. Instead, verification is required from everyone trying to access resources within the network, ensuring robust and granular security. Unlike traditional security models that rely on a trusted internal network and a less trusted external network, ZTA treats all network traffic as untrusted, continuously validating users and devices before granting

access to sensitive data and systems. This model significantly mitigates the risk of cyber threats by ensuring that access is granted only to those who genuinely need it and are properly authenticated.

In zero trust architecture, ***policy-based authentication*** is a crucial component. This approach ensures that all access requests are dynamically authenticated using pre-defined security policies that consider a variety of factors. These factors include the identity of the user, the device being used, the location of the access request, and the nature of the resource being accessed. Each access attempt is subjected to rigorous authentication checks, which may include multifactor authentication (MFA) and contextual data analysis. For instance, a user attempting to access a corporate resource from an unfamiliar location or device might be required to provide additional verification to ensure they are who they claim to be. By implementing policy-based authentication, ZTA enhances security by dynamically adjusting access requirements based on the context and potential risks associated with each request.

Once authentication is successfully achieved, ZTA moves to policy-based ***authorization***, which governs what authenticated users are permitted to do within the network. Authorization policies are designed to be granular and specific, ensuring that users have access only to the resources necessary for their roles and tasks. These policies are enforced in real time, continually reassessing user permissions based on their current context and behavior. For example, if a user's behavior deviates from their usual patterns, such as accessing sensitive data they don't typically handle, the system may prompt for additional verification or deny access altogether. This dynamic and context-aware approach to authorization helps prevent unauthorized access and reduces the risk of data breaches by ensuring that permissions are strictly aligned with business needs and security requirements.

Central to the ZTA model is the concept of ***least privilege access***. This principle dictates that users and devices should be granted the minimum level of access required to perform their functions and no more. By limiting access rights, ZTA minimizes the potential damage that could be caused by compromised credentials or malicious actors. Implementing least privilege access involves meticulously defining user roles, responsibilities, and the associated access permissions. For instance, a financial analyst may need access to financial records but not to customer personal information, while an IT administrator might need access to system logs but not to employee payroll data. Regular reviews and adjustments of access levels are also essential to accommodate changes in roles and responsibilities, ensuring that access permissions remain tightly controlled and aligned with the principle of least privilege access.

SASE and SSE

Secure Access Secure Edge (SASE) is a transformative architectural framework designed to meet the demands of modern networking and security. It is a cloud-native service model that converges wide area networking and network security services like Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS) into a single cloud-based service. This convergence allows organizations to securely connect users, devices, and applications over a global network. The SASE framework was first conceptualized by Gartner in 2019 as a response to the evolving IT landscape, where traditional network and security models were becoming increasingly insufficient for the dynamic, distributed, and cloud-centric environments.

At its core, SASE provides secure and optimized access to applications and resources regardless of the user's location. This is crucial in the current era where remote work and cloud adoption have surged, making traditional perimeter-based security models obsolete. SASE combines networking and security functionalities in a unified platform, delivered as a service from the cloud. This integration simplifies the complexity of managing multiple standalone solutions, reduces costs, and provides consistent security policies across all edges of the network, including data centers, branches, mobile users, and Internet of Things (IoT) devices.

A key aspect of SASE is its emphasis on zero trust security principles. Unlike traditional network security models that focus on defending a defined perimeter, zero trust assumes that threats can originate from both outside and inside the network. SASE implements zero trust by verifying the identity and integrity of users and devices before granting access to applications and data. This ensures that only authenticated and authorized entities can access sensitive resources, mitigating risks associated with internal and external threats. Furthermore, SASE continuously monitors and enforces security policies based on user behavior, device status, and network context to dynamically adapt to changing threat landscapes.

SASE also addresses the need for optimized network performance by integrating SD-WAN capabilities. By leveraging the global presence of SASE providers, organizations can benefit from reduced latency, improved application performance, and enhanced user experience, regardless of the user's geographical location.

SASE also supports a holistic approach to data protection and compliance. By consolidating security functions into a single framework, SASE provides comprehensive visibility and control over data flows across the network. This enables organizations to enforce data loss prevention (DLP) policies, detect and respond to threats in real time, and ensure compliance with regulatory requirements. The centralized management of security policies also simplifies the auditing process and facilitates the rapid implementation of policy changes to adapt to evolving compliance demands.

Security Service Edge (SSE) is a cloud-native cybersecurity framework that provides a comprehensive suite of security services to protect data, applications, and users in a distributed, cloud-centric environment. Introduced by Gartner as a distinct subset of the broader Secure Access Service Edge (SASE) model, SSE focuses specifically on delivering security services without encompassing the networking components such as SD-WAN. It is designed to address the challenges of modern IT architectures, where traditional perimeter-based security is inadequate for safeguarding against sophisticated cyber threats targeting a dispersed workforce and cloud-hosted resources.

SSE is particularly relevant in the context of today's hybrid and remote work environments, where employees access corporate resources from various locations and devices. Traditional security solutions that rely on a fixed perimeter are insufficient in such scenarios, as they cannot effectively protect against threats targeting remote users or cloud-hosted data. SSE addresses this challenge by extending security controls to the edge, ensuring that all users, regardless of their location, are subject to the same rigorous security policies. This approach not only improves security but also simplifies the management of security infrastructure by consolidating it into a single cloud-based service.

Another significant aspect of SSE is its focus on data protection and regulatory compliance. With the increasing volume of sensitive data being stored and processed in the cloud, organizations face greater risks of data breaches and regulatory fines. SSE helps mitigate these risks by providing advanced data protection capabilities such as encryption, data loss prevention, and threat detection. These features ensure that sensitive data is safeguarded against unauthorized access and exfiltration, and that organizations can maintain compliance with data privacy regulations like GDPR, CCPA, and HIPAA.

Infrastructure as Code (IaC)

One of the most exciting developments in technology today is **infrastructure as code (IaC)**. When your infrastructure (often in the cloud) is all virtualized, it can be easily created (and destroyed) as well as maintained by using scripts (code). This makes it possible for you to “spin up” test environments or pilot tests with ease. Think about how much easier it is to create a duplicate site for high availability (HA) needs when using IaaS and IaC than when using physical devices.

The large public cloud providers make it simple for you to implement IaC. They provide tools (such as CloudFormation from AWS) that permit you to easily generate the code required to script the creation of useful (and even complex) infrastructures. Thanks to this capability, you can easily automate—and even orchestrate—common networking tasks that used to take weeks or months to carry out.

For example, say that you need to spin up 50 servers for a test project. Thanks to IaC, you can now do this with a few clicks of the mouse instead of using a massive (and often) expensive deployment of physical servers.

There is a difference between automation and orchestration:

- **Automation** refers to the automated completion of a task or tasks.
- **Orchestration** refers to the scheduling and monitoring of many different automations. It is, basically, automating the automation.

NOTE IaC is also known as *programmable infrastructure* to indicate that the infrastructure configuration can be incorporated into application code. IaC enables DevOps teams to test applications in production-like environments from the beginning of the development cycle.

Key components of automation in IaC include playbooks, templates, and reusable tasks, which facilitate the creation, maintenance, and scaling of infrastructure in a consistent manner. Additionally, automation helps address challenges such as configuration drift, compliance, and upgrades, and supports dynamic inventories for flexible resource management. Here are more details on the key components and advantages of automation with IaC:

Key Topic

- **Playbooks:** Playbooks are a fundamental tool in IaC automation, particularly in tools like Ansible. They provide a structured way to define a series of tasks that automate the provisioning, configuration, and management of infrastructure. Playbooks are written in YAML and describe the desired state of the infrastructure in a declarative manner. This allows for complex workflows to be automated, such as deploying applications, configuring servers, and managing network devices.

NOTE Ansible is a software tool that enables infrastructure as code. It is open source and includes modules for software provisioning, configuration management, and application deployment functionality. YAML is a human-readable data serialization language. It is commonly used for configuration files and in applications where data is being stored or transmitted.

- **Templates:** Templates in IaC are used to define infrastructure resources in a reusable and consistent manner. Tools like Terraform and AWS CloudFormation utilize templates to describe cloud resources and their relationships. These templates can include variables, allowing for parameterization and flexibility in resource configurations. For example, a template might define a

virtual machine with specific attributes like instance type, security groups, and attached storage. By using templates, organizations can ensure that infrastructure components are created with a consistent configuration across different environments, reducing the risk of configuration errors and making it easier to replicate and scale infrastructure.

- **Reusable tasks:** Reusable tasks are a key aspect of IaC automation that promote efficiency and maintainability. In tools like Ansible, reusable tasks can be defined in roles, which are collections of tasks, variables, and templates organized in a structured format. Roles can be shared across multiple playbooks and projects, allowing for the reuse of common configurations and deployment steps. For example, a role might encapsulate the tasks required to set up a web server, including installing packages, configuring services, and managing firewall rules.
- **Configuration drift:** Configuration drift occurs when the actual state of the infrastructure deviates from the desired state defined in the IaC. This can happen due to manual changes, system updates, or environmental factors. Automation in IaC helps mitigate configuration drift by regularly applying the desired state to the infrastructure. Tools like Terraform and Ansible can perform periodic checks and reapply configurations to ensure consistency. This not only helps maintain the reliability and predictability of the infrastructure but also reduces the time and effort required to troubleshoot and resolve issues caused by drift. Automation ensures that the infrastructure remains aligned with the defined state, minimizing the risks associated with unintended changes.
- **Compliance:** Compliance with industry standards and regulatory requirements is a critical aspect of infrastructure management. Automation in IaC enables organizations to enforce compliance by embedding policies and controls directly into the infrastructure code. For example, security configurations, access controls, and data protection measures can be defined in the IaC templates and playbooks. Automated tools can continuously monitor the infrastructure for compliance with these policies, generating reports and alerts when deviations occur.
- **Upgrades:** Upgrading infrastructure components, such as software versions, operating systems, and hardware configurations, can be a complex and error-prone process. IaC automation simplifies upgrades by allowing organizations to define the desired state of the infrastructure, including the required versions and configurations. Upgrades can be tested in a staging environment using the same IaC definitions before being applied to production, reducing the risk of disruptions.

- **Dynamic inventories:** Dynamic inventories are a feature of IaC automation that allows the infrastructure to be dynamically discovered and managed based on current configurations and states. This is particularly useful in cloud environments, where resources can be created and terminated frequently. Tools like Ansible support dynamic inventories, which can query cloud providers or other data sources to generate an up-to-date list of resources for configuration management tasks.

Because the C in IaC stands for code, it is of no surprise that IaC systems tend to take advantage of **source control** systems. These systems tend to feature the following:

- **Version control:** Version control is at the heart of source control systems and is vital for managing IaC. It enables teams to track changes to infrastructure code over time, maintaining a history of modifications, additions, and deletions. Each change is recorded with a unique identifier, often called a *commit*, along with metadata such as the author, timestamp, and a message describing the change.
- **Central repository:** A central repository in a source control system acts as the single source of truth for all infrastructure code. This repository stores the master copies of the code and provides a central location where all team members can access, contribute to, and collaborate on the infrastructure codebase.
- **Conflict identification:** Conflict identification is an essential feature of source control systems, especially in collaborative IaC environments, where multiple team members may work on the same code simultaneously. Conflicts occur when changes made by different users overlap or are incompatible with each other.
- **Branching:** Branching is a powerful feature of source control systems that allows teams to create isolated copies of the codebase for different purposes. This is particularly useful in IaC environments for managing multiple streams of development and experimentation without affecting the main codebase.

IP Version 6

With the global proliferation of IP-based networks, available IPv4 addresses are rapidly becoming exhausted. Fortunately, IPv6 provides enough IP addresses for many generations to come. This section introduces **IPv6 addressing** with a deep dive into IPv6's address structure and a discussion of some of its unique characteristics.

Need for IPv6

With the worldwide depletion of IP version 4 (IPv4) addresses, many organizations have migrated, are in the process of migrating, or are considering migrating their IPv4 addresses to IPv6 addresses. IPv6 dramatically increases the number of available IP addresses. In fact, IPv6 offers approximately 5×10^{28} IP addresses for each person on the planet.

Beyond the increased address space, IPv6 offers many other features:

- Simplified header:
 - The IPv4 header uses 12 fields.
 - The IPv6 header uses 5 fields.
- No broadcasts
- No fragmentation (performs MTU discovery for each session)
- Can coexist with IPv4 during a transition:
 - **Dual stack** (running IPv4 and IPv6 simultaneously on a network interface or device)
 - IPv6 over IPv4 (tunneling IPv6 over an IPv4 tunnel)

Even if you are designing a network based on IPv4 addressing, it is a good practice to consider how readily an IPv6 addressing scheme could be overlaid on that network at some point in the future. Using Teredo **tunneling**, an IPv6 host could provide IPv6 connectivity even when the host is directly connected to an IPv4-only network. Miredo is a client that can be used to implement the Teredo protocol and is included in many versions of Linux. IPv6/IPv4 tunneling is often referred to as 6to4 or 4to6 tunneling, depending on which protocol is being tunneled (IPv4 or IPv6). These are just some of the many tunneling mechanisms devised to ensure a smooth transition from IPv4 to IPv6. In fact, thanks to dual stack and tunneling features, it is very unlikely that you will see IPv4 ever completely go away in your lifetime.

Since there are so many available IPv6 addresses, network address translation (NAT) is not nearly as required in IPv6. One way it can be useful is in transition between the two versions, however. Network address translation from IPv6 to IPv4 (**NAT64**) is a technology that facilitates communication between IPv6-only clients and IPv4-only servers, bridging the gap between the two distinct IP address families. It is yet another component in the transition from the older IPv4 protocol to the newer IPv6 protocol, allowing IPv6 networks to access resources on IPv4 networks without requiring the end systems to support both protocols. NAT64 works by translating

IPv6 packets to IPv4 packets and vice versa, using a predefined prefix to generate an IPv6 address that maps to an IPv4 address.

IPv6 Address Structure

An IPv6 address has the following address format, where *X* is a hexadecimal digit in the range of 0 to F:

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

A hexadecimal digit is 4 bits in size (4 binary bits can represent 16 values). Notice that an IPv6 address has eight fields, and each field contains four hexadecimal digits. The following formula reveals why an IPv6 address is a 128-bit address:

$$4 \text{ bits per digit} \times 4 \text{ digits per field} \times 8 \text{ fields} = 128 \text{ bits in an IPv6 address}$$

IPv6 addresses can be difficult to work with because of their size. Fortunately, the following rules (often collectively referred to as *shorthand notation*) exist for abbreviating these addresses:

- Leading 0s in a field can be omitted.
- Contiguous fields containing all 0s can be represented with a double colon. (Note that this can be done only once for a single IPv6 address.)

For example, consider the following IPv6 address:

ABCD:0123:4040:0000:0000:000A:000B

Using the rules for abbreviation, the IPv6 address can be rewritten as follows:

ABCD:123:4040::A:B

An exciting feature of IPv6 is the Extended Unique Identifier (EUI-64) format, which permits a device to automatically populate the low-order 64 bits of an IPv6 address based on an interface's MAC address. You will read more about this capability later in this chapter.

IPv6 Address Types

The following are some of the many unique aspects of IPv6 addressing and interesting address types:

- IPv6 globally routable unicast addresses start with the first four hex characters in the range 2000 to 3999.
- An IPv6 link-local address is also used on each IPv6 interface. The link-local address begins with FE80.

- Multicast addresses begin with FF as the first two hex characters.
- IPv6 can use autoconfiguration to discover the current network and select a host ID that is unique on that network. Automatic generation of a unique host ID is made possible through a process known as *EUI-64*, which uses the 48-bit MAC address on the device to aid in the generation of the unique 64-bit host ID. Notice that the autoconfiguration capabilities described here permit you to create an IPv6 network free of DHCP-type services. The ability of IPv6 to replace the need for DHCP services like this is known as stateless address autoconfiguration (SLAAC). You will learn more about SLAAC in Chapter 16, “IPv4 and IPv6 Network Services.”
- IPv6 can also use a special version of DHCP for IPv6. Not surprisingly, this version is called *DHCPv6*.
- The protocol that is used for *network discovery*—that is, to discover the network address and learn the Layer 2 addresses of neighbors on the same network—is Neighbor Discovery Protocol (NDP).

NDP is hugely important in IPv6. It defines five ICMPv6 packet types for important jobs:

- Key Topic**
- **Router Solicitation:** Hosts inquire with Router Solicitation messages to locate routers on an attached link.
 - **Router Advertisement:** Routers advertise their presence together with various link and Internet parameters, either periodically or in response to a Router Solicitation message.
 - **Neighbor Solicitation:** Neighbor solicitation messages are used by nodes to determine the link layer address of a neighbor or to verify that a neighbor is still reachable via a cached link layer address.
 - **Neighbor Advertisement:** Neighbor advertisement messages are used by nodes to respond to a Neighbor Solicitation message.
 - **Redirect:** Routers may inform hosts of a better first-hop router for a destination.

IPv6 Data Flows

You might recall from our discussion of IPv4 traffic flows in Chapter 4 that there are unicast, broadcast, multicast, and anycast methods of communication possible with IP version 4. IPv6 uses just three of the four types of data flows:

Key Topic

- Unicast
- Multicast
- Anycast

Just like in IPv4, IPv6 uses special address types for these data flows. The following sections summarize the characteristics of each address type.

Unicast

With unicast, a single IPv6 address is applied to a single interface, as illustrated in Figure 8-3. The communication flow can be thought of as a one-to-one communication flow.

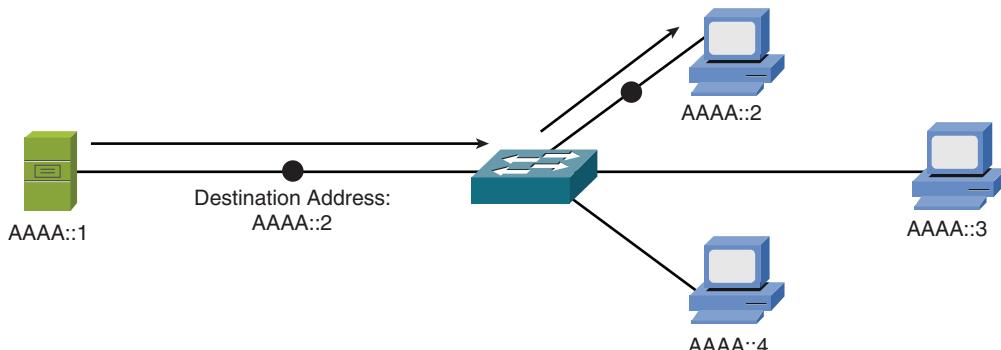


Figure 8-3 IPv6 Unicast Example

In Figure 8-3, a server (AAAA::1) is sending traffic to a single client (AAAA::2).

Multicast

With multicast, a single IPv6 address (a multicast group) can represent multiple devices on a network, as shown in Figure 8-4. The communication flow is a one-to-many communication flow.

In Figure 8-4, a server (AAAA::1) is sending traffic to a multicast group (FF00::A). Two clients (AAAA::2 and AAAA::3) have joined this group. Those clients receive the traffic from the server, and any client that did not join the group (for example, AAAA::4) does not receive the traffic.

IPv6 replaces broadcast behavior with multicast, thanks to the “all nodes” multicast group. This reserved address is FF01:0:0:0:0:0:1 (FF01::1). All IPv6 nodes join this group. This is a simple and efficient method for sending traffic to all nodes.

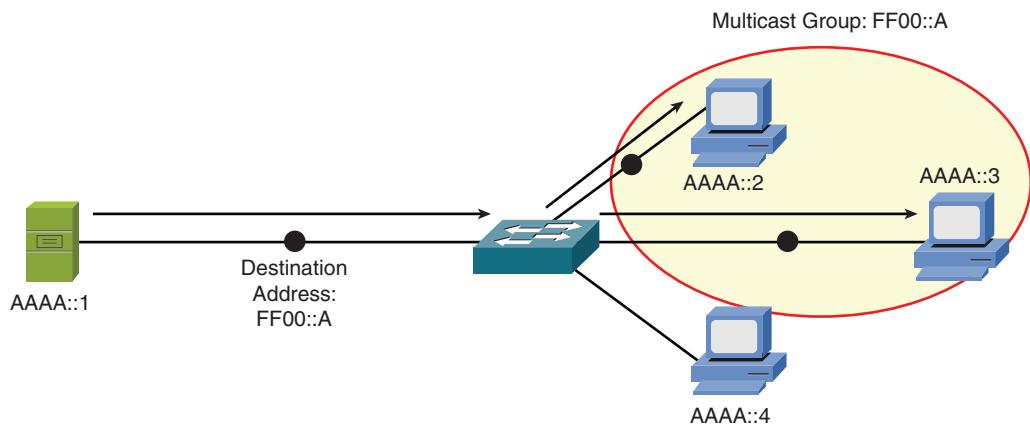


Figure 8-4 IPv6 Multicast Example

Anycast

With *anycast*, a single IPv6 address is assigned to multiple devices, as illustrated in Figure 8-5. It is a one-to-nearest (from the perspective of a router's routing table) communication flow.

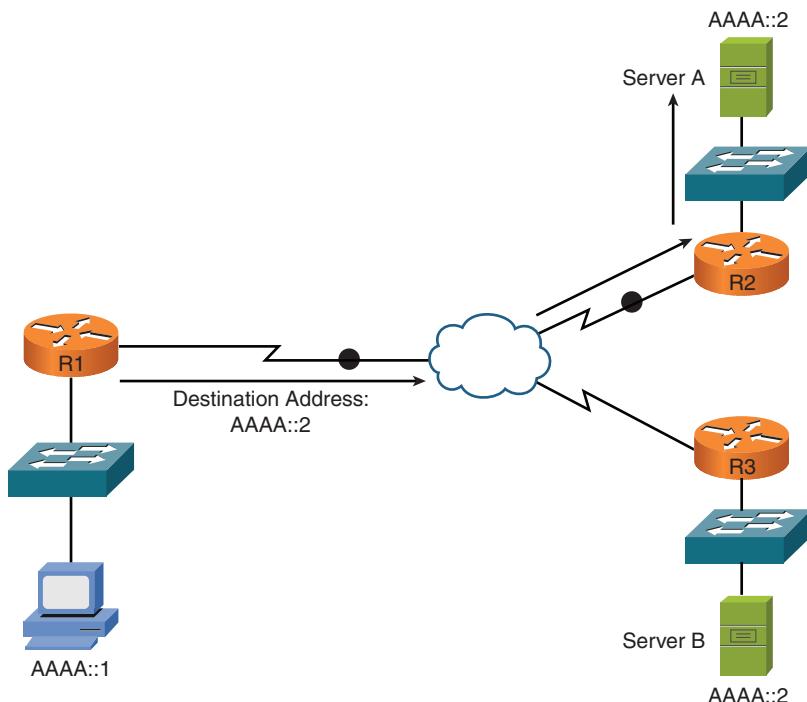


Figure 8-5 IPv6 Anycast Example

In Figure 8-5, a client with IPv6 address AAAA::1 wants to send traffic to destination IPv6 address AAAA::2. Notice that two servers (Server A and Server B) have the IPv6 address AAAA::2. In the figure, the traffic destined for AAAA::2 is sent to Server A, via router R2, because the network on which Server A resides appears to be closer than the network on which Server B resides, from the perspective of router R1's IPv6 routing table.

NOTE Remember that the dreaded broadcast frames and packets from IPv4 do not exist in an IPv6-only network. IPv6 uses only unicasts, multicasts, and anycasts, as described in this section. With IPv6, if you want to send a frame or packet to all nodes in the local network, you use the all-nodes IPv6 multicast address.

Real-World Case Study

Acme, Inc. is currently investigating the use of a software-defined wide area network (SD-WAN) to help revolutionize the legacy WAN infrastructure. Specifically, Acme is very interested in the enhanced network performance that this solution can bring. Acme would like the SD-WAN solution to dynamically route traffic over the best available path based on real-time network conditions, such as latency, jitter, and packet loss. This would ensure that critical applications, like video conferencing and cloud services, receive the bandwidth and low-latency routes they need, resulting in a better user experience.

Acme, Inc. is also actively exploring the implementation of a new zero trust architecture to enhance its cybersecurity posture and mitigate the risks associated with modern cyber threats. Unlike traditional security models that rely on a defined network perimeter, zero trust operates on the principle that no user or device, whether inside or outside the network, should be trusted by default. This approach aligns with Acme's goal of protecting sensitive data and resources in an increasingly complex and distributed IT environment. By adopting zero trust, Acme can ensure that all access requests are continuously verified and authenticated, regardless of the user's location or network. This is particularly important as Acme's workforce becomes more mobile and remote, accessing company resources from various devices and locations. Zero trust will enable Acme to enforce strict access controls and minimize the attack surface, thereby reducing the likelihood of unauthorized access and data breaches.

The move toward zero trust is also driven by Acme's desire to streamline compliance with regulatory requirements and enhance the overall resilience of its IT infrastructure. Zero trust architecture provides a comprehensive framework for implementing security policies that are consistent and enforceable across all endpoints and applications. This allows Acme to achieve greater visibility into user activities and data flows, ensuring that any suspicious behavior is promptly detected and addressed. Additionally, the granular control afforded by zero trust helps Acme to safeguard sensitive information and comply with regulations such as GDPR and HIPAA, which mandate stringent data protection measures. By integrating zero trust principles into its security strategy, Acme aims to build a robust and adaptable security model that not only protects against current threats but also evolves to address future challenges, ultimately supporting the company's growth and operational excellence.

Summary

Here are the main topics covered in this chapter:

- This chapter first provided a description of software-defined networking (SDN) and software-defined wide area networks (SD-WAN).
- This chapter next covered emerging technology of Virtual Extensible Local Area Networks (VXLAN). After describing the Layer 2 encapsulation that makes this technology function, this section described the common use case of the data center interconnect (DCI) functionality.
- This chapter then examined the emerging technology of the zero trust architecture (ZTA), including its major components of policy-based authentication, authorization, and least privilege access.
- This chapter defined the Secure Access Secure Edge (SASE) and Security Service Edge (SSE) solutions.
- This chapter covered the concept of infrastructure as code (IaC) and emphasized the features of IaC that rely on automation. This section of the chapter also discussed how source control can be critical to the IaC environment.
- The characteristics of IPv6 were highlighted, including the IPv6 address format and IPv6 data flows (unicast, multicast, and anycast).

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-1 lists these key topics and the page number where each is found.

Table 8-1 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Section	Software-Defined Networking (SDN)	205
Section	Virtual Extensible Local Area Network (VXLAN)	208
Section	Zero Trust Architecture (ZTA)	209
List	Key components for IaC	213
List	Steps for shorthand with IPv6 addresses	217
List	Functions of NDP	218
List	Types of IPv6 data flows	219

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

application awareness, authorization, automation, branching, central policy management, central repository, compliance, configuration drift, conflict identification, data center interconnect (DCI), dual stack, dynamic inventories, infrastructure as code (IaC), IPv6 addressing, Layer 2 encapsulation, least privilege access, NAT64, playbooks, policy-based authentication, reusable tasks, Secure Access Secure Edge (SASE), Security Service Edge (SSE), source control, software-defined networking (SDN), software-defined wide area network (SD-WAN), templates, transport agnostic, tunneling, upgrades, version control, Virtual Extensible Local Area Network (VXLAN), zero-touch provisioning (ZTP), zero trust architecture (ZTA)

Additional Resources

Software Defined Networking (SDN) Demystified: <https://www.youtube.com/watch?v=lVcUZCVvBjw>

VXLAN Simple Explanation: <https://www.youtube.com/watch?v=7Shfu9BrJP8>

Review Questions

The answers to these review questions appear in Appendix A, “Answers to Review Questions.”

1. BGP is an example of a technology found in what layer/plane of operation in a software-defined network?
 - a. Management
 - b. Control
 - c. Data
 - d. Application
2. What feature of the SD-WAN allows the network to seamlessly route and manage traffic over diverse transport media without dependency on the underlying physical connections?
 - a. Central policy management
 - b. Application awareness
 - c. Zero-touch provisioning
 - d. Transport agnostic
3. What protocol serves as the transport protocol for encapsulating Layer 2 Ethernet frames with Layer 3 packets in the VXLAN solution?
 - a. UDP
 - b. TCP
 - c. ARP
 - d. FHRP

4. What is the term given to the difference in the actual state of your infrastructure compared to the state defined in an IaC implementation?

- a. Version control
- b. Configuration drift
- c. Source control
- d. Conflict identification

5. How can the following IPv6 address be condensed?

2009:0123:4040:0000:0000:000A:100B

- a. 2009::123:404:A:100B
- b. 2009::123:404:A:1B
- c. 2009:123:4040::A:100B
- d. 2009:0123:4040::0::000A:100B

6. What technology allows for the automatic assignment of the host portion of an IPv6 address?

- a. Dual stack
- b. EUI-64
- c. Neighbor discovery
- d. Anycast

7. What can IPv6 networks use to assign IP addresses?

- a. SLAAC
- b. CIDR
- c. Port address translation
- d. Classless inter-domain routing notation

8. Which of the following is a network architecture that integrates wide area networking (WAN) capabilities with comprehensive network security functions such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Zero Trust Network Access (ZTNA)?

- a. SD-WAN
- b. VXLAN
- c. SSE
- d. SASE

9. Which of the following involves connecting multiple data centers to provide a unified infrastructure, allowing for efficient resource sharing, workload mobility, and disaster recovery?
 - a. NAT64
 - b. SASE
 - c. DCI
 - d. SSE

10. Which of the following is a technology that facilitates communication between IPv6-only clients and IPv4-only servers, bridging the gap between the two distinct IP address families?
 - a. NAT64
 - b. Dual stack
 - c. Conflict identification
 - d. Branching

This page intentionally left blank

Index

Numerics

2.4GHz band, 102–104
3DES (Triple DES), 427
5GHz band, 104, 292
6GHz band, 292
10BASE2, 122–123
10BASE5, 122–123
10BASE-T, 123–124
66 block, 313
100BASE-T, 126
100BASE-TX, 126
110 block, 313–314
802.1Q, 267
802.1X, 301–302, 416
802.11a, 106
802.11ac, 107
802.11ax, 102, 107–108
802.11b, 106
802.11g, 106
802.11h, 292
802.11n, 106–107
802.3. *See* Ethernet
802.3af, 278
1000BASE-X, 126

A

AAA (authentication, authorization, and accounting), 416
access control, role-based, 434
access/edge layer, three-tier hierarchical model, 150–151
acknowledgment number field, 24

ACL (access control list), troubleshooting, 521
AD (administrative distance), 237
ad hoc WLAN, 286, 293
address translation, 244
 NAT (network address translation), 244–246
 PAT (port address translation), 246–248
advanced distance-vector routing protocol, EIGRP (Enhanced Interior Gateway Routing Protocol), 242–243
advanced subnetting, 192–196
AES (Advanced Encryption Standard), 428
AH (Authentication Header), 410–413
algorithm
 asymmetric encryption, 428–429
 Dijkstra's shortest path first, 242
 hashing, 345, 430–431
 security, 345
 symmetric encryption, 427–428
AM (amplitude modulation), 8
amplified attack, 458
anomaly alerting, 348
anomaly-based IDS/IPS, 48–49
antenna, 289–290
 gain, 290
 omnidirectional, 290–291
 polarity, 292
troubleshooting, 533
unidirectional, 291

- anycast transmission, 92–93, 220–221
- AP (access point), 52–53, 287–289
 - association, 287
 - autonomous, 53, 288
 - band steering, 293
 - lightweight, 53, 288–289
 - placement, 296–301
 - roaming, 297
 - rogue, 300, 461
 - signal strength, 297
- API (application programming interface), 354–355, 415
- APIPA (Automatic Private IP addressing), 180–181
- application awareness, SD-WAN
 - (software-defined wide area network), 207
- application layer
 - OSI model, 21–24
 - TCP/IP stack, 25
- application plane, SDN (software-defined networking), 205
- APT (advanced persistent threat), 468
- ARIN (American Registry for Internet Numbers), 174
- ARP (Address Resolution Protocol), 263
 - poisoning, 460
 - spoofing, 459
- arp command, 558–560
- ARPANET, 22
- ASCII (American Standard Code for Information Interchange), 20, 68–69
- assessment
 - posture, 442
 - process, 443
 - risk, 442
 - threat, 442
 - vendor, 443
 - vulnerability, 442
- asset
 - inventory, 327
- tracking tag, 444
- association, 287
- asymmetric encryption, 428–430
- asynchronous transmission, 13
- attack/s
 - APT (advanced persistent threat), 468
 - birthday, 468
 - bluejacking, 469
 - bluesnarfing, 469
 - buffer overflow, 467
 - confidentiality, 465
 - cryptojacking, 468
 - data diddling, 467
 - downgrade, 468
 - EMI interception, 465
 - fileless malware, 468
 - FTP bounce, 466
 - ICMP, 467–468
 - information sent over covert channels, 466
 - information sent over overt channels, 466
 - keylogger trojan, 468
 - LDAP injection, 469
 - logic bomb, 467
 - packet capture, 465
 - password spraying, 468
 - privilege escalation, 469
 - salamis, 466
 - session hijacking, 466
 - skimming, 468
 - social engineering, 463–464
 - dumpster diving, 464
 - phishing, 464
 - piggybacking, 464
 - shoulder surfing, 464
 - tailgating, 464
 - SQL injection, 468
 - supply chain, 468
 - TCP SYN flood, 467
 - technology-based ARP poisoning, 460

- ARP spoofing, 461
 - DDoS (distributed denial-of-service), 459
 - deauthentication, 463
 - DNS poisoning, 460
 - DoS (denial-of-service), 458–459
 - evil twin, 461
 - IP spoofing, 463
 - MAC flooding, 462
 - MAC spoofing, 462
 - malware, 463–465
 - password, 462
 - on-path, 459–460
 - ransomware, 461
 - rogue access point, 461
 - rogue DHCP servers, 461
 - VLAN hopping, 460
 - trust relationship exploitation, 467
 - USB drop, 468
 - wiretapping, 465
 - zero-day, 432
 - attenuation, 503, 532
 - authentication
 - de-, 463
 - Kerberos, 440
 - local, 417, 441
 - multifactor, 417, 438–439, 448
 - policy-based, 212–213
 - RADIUS (Remote Authentication Dial-In User Service), 439
 - SAML (Security Assertion Markup Language), 441
 - SSO (single sign-on), 439
 - TACACS+ (Terminal Access Controller Access-Control System), 439
 - time-based, 441
 - two-factor, 417
 - authorization, 210, 433
 - automation, 213
 - IaC (infrastructure as code)
 - playbook, 213
 - reusable tasks, 214
 - upgrades, 214
 - autonomous AP, 53, 288
 - availability, 431. *See also* high availability
 - five nines, 364, 431
 - high, 364
 - monitoring, 356
 - AWS
 - Direct Connect, 73
 - IAM (Identity and Account Management), 433
 - SG (security group), 69
 - VPC (virtual private cloud), 67–68
- B**
- backup
 - differential, 369
 - full, 369
 - incremental, 369
 - snapshot, 369
 - backup configuration, 333
 - badge reader, 446
 - in-band network management, 418
 - band steering, 293
 - bandwidth, 9–10, 55, 57, 124, 347, 530
 - Ethernet, 124–125, 263–264
 - speed tester, 544
 - baseband, 10
 - baseline configuration, 334–335
 - baseline metric, 347
 - basic PDU (power distribution unit), 315
 - best match, 233
 - BGP (Border Gateway Protocol), 243, 250
 - binary numbers, 164
 - converting to decimal, 164–165, 167–168
 - octet, 164
 - biometrics, 446
 - birthday attack, 468
 - bit/s, 8, 124
 - parity, 14
 - synchronization, 9

- BIX (Building Industry Cross-connect),
314
- bluejacking, 469
- bluesnarfing, 469
- BNC (Bayonet Neill-Concelman) connector, 112
- BOOTP (Bootstrap Protocol), 386
- bots, 459
- bottlenecks, 530
- BPDU (bridge protocol data unit), 273
- broadband, 9
- broadcast storm, 270–271
- broadcast transmission, 91
- brute-force attack, 462
- BSSID (basic service set identifier), 300
- buffer overflow, 467
- buffering, 18–19
- bug fix, 330
- BYOD (bring your own device), 523
- C**
- cable, 128
- 66 block, 313
 - 110 block, 313–314
 - attenuation, 503, 532
 - Cat6a, 318
 - coaxial, 1112
 - BNC connector, 112
 - F-connector, 112–113
 - crimper, 507
 - crossover, 116, 268
 - direct attach copper, 113
 - distribution system, 310–312
 - EMI (electromagnetic interference), 318, 503
 - fiber-optic, 117–118
 - connector polishing styles, 121
 - connectors, 120–121
 - MMF, 118–120
 - multiplexing, 127
 - patch panel, 313
 - SMF, 120
- IDF (intermediate distribution frame),
313
- maps and diagrams, 326
- MDF (main distribution frame),
314–315
- open, 504
- patch panel, 312
- plenum, 117, 503
- riser, 503
- speed, 115
- straight-through, 115
- stripper, 511
- tester, 569
- troubleshooting, 531–533
- twinax, 112
- twisted pair, 113
 - shielded, 113–114
 - unshielded, 114–116
- cable modem, 9
- camera, surveillance, 444
- CAN (campus area network), 139
- captive portal, 289, 417, 481
- CARP (Common Address Redundancy Protocol), 249
- Cat6a cable, 318
- CDN (content delivery network), 54
- CDP (Cisco Discovery Protocol), 547
- cell, WLAN, 297
- cellular, 108–109
- center frequency, 105
- central policy management, 208
- change management, 332–333
 - documentation, 333–334
 - request process tracking, 332
 - service requests, 332
- channel/s, 102–103
 - bonding, 107
 - center frequency, 105
 - width, 292
- checksum, 13
- child tunnel, 413

- CIA (confidentiality, integrity, and availability)
 - availability, 431
 - confidentiality, 426–430
 - integrity, 430–431
- CIDR (classless inter-domain routing), 196–197
- circuit switching, 15
- Cisco ACI (Application Centric Infrastructure), 153–154
- clientless VPN, 407
- client/server network, 140–141
- client-to-site VPN, 406
- cloud, 75
 - community, 71
 - connectivity options, 73
 - DaaS (desktop as a service), 73
 - elasticity, 74
 - gateway, 69–71
 - hybrid, 71
 - hybrid cloud, 72
 - IaaS (infrastructure as a service), 72
 - multitenancy, 74
 - network security group, 68–69
 - network security list, 69
 - NFV (network functions virtualization), 66
 - PaaS (platform as a service), 72
 - private, 71, 72
 - providers, 68
 - public, 71, 72
 - SaaS (software as a service), 72
 - scalability, 75
 - service models, 72–73
 - virtual private, 67–68
- cluster, server, 368
- CMA (code-division multiple access), 109
- coaxial cable, 1112
 - BNC connector, 112
 - F-connector, 112–113
- code, infrastructure as, 212–213
- cold site, 371
- collapsed core design, 152
- collision, Ethernet, 258–260
- collision domain, 36
 - CSMA/CA (carrier-sense multiple access with collision avoidance), 260
 - CSMA/CD (carrier-sense multiple access with collision detection), 258–262
- command and control software, 459
- command/s
 - arp, 558–560
 - dig, 556–557
 - hostname, 562
 - ifconfig, 553–554
 - ip, 554
 - ipconfig, 549–553
 - netstat, 560–562
 - nmap, 567
 - nslookup, 554–556
 - ping, 547–549
 - port, 466
 - route, 562–567
 - show, 567–568
 - switchport port-securit, 266–267
 - tcpdump, 567
 - telnet, 567
 - traceroute, 557–558
- community cloud, 71
- community strings, SNMP, 343
- compliance, regulatory, 447–448
- CompTIA Network+ N10-009 exam
 - preparation
 - strategies for taking the exam, 581–582
 - suggested plan for final review and study, 579–581
 - tools for final preparation, 577–578
- computer cluster, 367–368
- confidentiality, 426–430, 465. *See also* encryption
- configuration
 - drift, 214

- management, 333–334
 - monitoring, 357
 - snapshot, 369
 - congestion, 530
 - connection services, network layer, 16
 - connectionless protocol, 27, 88
 - connection-oriented protocol, 88
 - connectivity
 - cloud, 73
 - troubleshooting, 490
 - connector
 - BNC (Bayonet Neill-Concelman), 112
 - fiber-optic, 120–121
 - short, 504
 - twisted-pair cable, 116–117
 - console, 415
 - content caching, 370
 - content switching, 370–371
 - contention, 530
 - control plane, SDN (software-defined networking), 207–208
 - convergence, 52, 55, 137
 - binary-to-decimal, 167–168
 - routing, 236
 - conversion
 - binary-to-decimal, 164–165
 - decimal-to-binary, 165–167, 168–170
 - CoPP (control plane policing), 479
 - core layer, three-tier hierarchical model, 152
 - COTS (commercial off-the-shelf) server, 66
 - CPU usage, 346
 - CRC (cyclic redundancy check), 14, 278, 505
 - crossover cable, 116, 268
 - cryptojacking, 468
 - CSMA/CA (carrier-sense multiple access with collision avoidance), 260
 - CSMA/CD (carrier-sense multiple access with collision detection), 258–262
 - current state modulation, 8
 - CVE (Common Vulnerabilities and Exposures), 432
 - CVSS (Common Vulnerability Scoring System), 432
 - CWDM (coarse wavelength-division multiplexing), 127
 - CYOD (choose your own device), 438
- D**
- DaaS (desktop as a service), 73
 - DAC (direct attach copper) cable, 113
 - DAI (dynamic ARP inspection), 462, 479
 - data
 - diddling, 467
 - locality, 447
 - at rest, 427
 - in transit, 427
 - data link layer, OSI model, 11–12
 - LLC (Logical Link Control) sublayer, 13–14
 - MAC (media access control) sublayer, 12
 - data plane, SDN (software-defined networking), 206
 - dB (decibel), 290, 504
 - DB-9 connector, 117
 - DCI (data center interconnect), 209
 - DDoS (distributed denial-of-service) attack, 459
 - deauthentication, 463
 - decapsulation, 4–5, 28
 - decimal numbers, converting to binary, 165–167, 168–170
 - default gateway, 175, 248
 - default route, 518
 - default static route, 234
 - default VLAN, 479
 - defense in depth, 434
 - delay, 56, 110
 - DES (Data Encryption Standard), 427
 - device. *See also* routers and routing; switches and switching

- bring your own, 523
- configuration, 518
- hardening, 476–480
- LED status indicators, 504
- update, 477
- DHCP (Dynamic Host Configuration Protocol), 83, 386, 399
 - client configuration, 388
 - components, 390
 - exclusive range, 388
 - messages, 386–387
 - relay, 387–389
 - reservation, 388
 - rogue server, 461
 - scope, 388
 - server, 388–389
 - snooping, 478
- diagram
 - cable, 326
 - network, 327
 - physical versus logical, 326
 - rack, 326
- dictionary password attack, 462
- differential backup, 369
- dig command, 556–557
- digital certificate, 429
- Dijkstra’s shortest path first, 242
- directly connected routes, 233
- disaster recovery
 - fault tolerance, 365–366
 - MTTR (mean time to repair), 364
 - RPO (recovery point objective), 365
 - RTO (recovery time objective), 365
 - testing, 372–373
- distance vector routing protocol, 239–241
- distribution/aggregation layer
 - MTBF (mean time between failure), 364
 - three-tier hierarchical model, 151–152
 - DLP (data loss prevention), 211, 417–418
 - DMZ (demilitarized zone), 435
 - DNAT (Dynamic NAT), 246
- DNS (Domain Name System), 27, 83, 391
 - dynamic, 394
 - Extension Mechanisms for, 394
 - forward lookup zone, 395
 - FQDN (fully qualified domain name), 391–392
 - global hierarchy, 392
 - IPAM (IP address management), 394
 - iterative lookup, 396
 - lookup, 38
 - over HTTPS, 396
 - over TLS, 396
 - poisoning, 460
 - primary zone, 395
 - records, 393
 - recursive lookup, 396
 - reverse lookup zone, 396
 - secondary zone, 395
 - servers, 392
 - TTL (Time-to-Live), 395
 - zone transfer, 394
- documentation, 326
 - asset inventory, 327
 - cable maps and diagrams, 326
 - change management, 333–334
 - IP address management, 328
 - network diagram, 327
 - physical and logical diagrams, 326
 - postmortem report, 495
 - rack diagram, 326
 - SLA (service-level agreement), 328
 - wireless survey/heat map, 328–329
- DoS (denial-of-service) attack, 458–459
- downgrade attack, 468
- drops, 56, 506
- DSSS (direct-sequence spread spectrum), 105
- dumpster diving, 464
- DWDM (dense wavelength-division multiplexing), 127
- dynamic addressing, 386

DHCP (Dynamic Host Configuration Protocol), 386

- client configuration, 388
- components, 390
- exclusive range, 388
- messages, 386–387
- relay, 387–389
- reservation, 388
- scope, 388
- server, 388–389

SLAAC (stateless address autoconfiguration), 389–390

- dynamic configuration, IPv4, 180
- dynamic DNS, 394
- dynamic inventories, IaC (infrastructure as code), 215
- dynamic routing protocols, 243–244

E

EAP (Extensible Authentication Protocol), 416, 481

- east-west traffic flow, 155
- EBCDIC (Extended Binary Coded Decimal Interchange Code), 20
- EDNS (Extension Mechanisms for DNS), 394
- EGP (exterior gateway protocol), 238
- EIGRP (Enhanced Interior Gateway Routing Protocol), 242–243
- EIRP (effective isotropic radiated power), 532
- elasticity, 74
- electrical disturbance attack, 467–468
- EMI (electromagnetic interference), 318, 465, 503
- employee training, 445–446
- encapsulation, 4–5
- encryption, 21
 - asymmetric, 428–430
 - symmetric, 427–428
- environmental monitors, 346

EOL (end-of-life), 330

EOS (end-of-support), 330

equipment. *See also* physical installation rack

- diagram, 326
- humidity levels, 317–318
- lockable, 315
- port-side exhaust and intakes, 315
- size, 314
- temperature control, 317

ESP (Encapsulating Security Payload), 410–413

ESS (extended service set), 295

ESSID (extended service set identifier), 300

Ethernet, 258–259

- 10BASE2, 122–123
- 10BASE5, 122–123
- 10BASE-T, 123–124

- bandwidth, 124–125
- collision, 258–260
- crossover cable, 116

- CSMA/CA (carrier-sense multiple access with collision avoidance), 260

- CSMA/CD (carrier-sense multiple access with collision detection), 258–262

- distance and speed limitations, 263–264

- Fibre Channel over, 52

- full-duplex mode, 262

- half-duplex mode, 262

- Power over, 277–278

- shared bus topology, 258

- types of, 125–126

- VLAN (virtual LAN), 263–265

EU (European Union), GDPR (General Data Protection Regulation), 448

Event Viewer, 353

evil twin, 461

exploit, 433

F

fault tolerance, 365–366
 FCoE (Fibre Channel over Ethernet), 52
 F-connector, 112–113
 FDM (frequency-division multiplexing), 10
 FHRP (First Hop Redundancy Protocol), 248, 249, 250
 CARP (Common Address Redundancy Protocol), 249
 GLBP (Gateway Load Balancing Protocol), 249
 HSRP (Hot Standby Router Protocol), 248–249
 VRRP (Virtual Router Redundancy Protocol), 249
 FHSS (frequency-hopping spread spectrum), 105
 fiber light meter, 511
 fiber-optic cable, 117–118
 connectors, 120–121
 MMF (multimode fiber), 118–120
 patch panel, 313
 SMF (single-mode fiber), 120
 troubleshooting, 505
 fileless malware, 468
 fire suppression, 318–319
 firewall, 45
 next-generation, 57
 rules, 480
 stateful, 45
 firmware, upgrade, 477
 five nines availability, 269, 364, 431
 flow control, 13, 16
 flow data, 354
 FM (frequency modulation), 8
 forward lookup zone, 395
 FQDN (fully qualified domain name), 175, 391–392
 frame, jumbo, 51. *See also* packet/s
 FTP (File Transfer Protocol), 82, 466

full backup, 369
 full tunnel VPN, 407
 full-duplex mode, 262
 full-mesh topology, 147–148
 fusion splicer, 511

G

gain, 290
 gateway
 cloud, 69–71
 default, 175, 248
 Internet, 70
 NAT (network address translation), 71
 GBIC (gigabit interface converter), 126
 GDPR (General Data Protection Regulation), 448
 geofence, 304, 447, 481–482
 giants, 506
 GLBP (Gateway Load Balancing Protocol), 249
 global hierarchy, DNS (Domain Name System), 392
 global routing table, 436
 golden configuration, 334–335
 GPG (GNU Privacy Guard), 428
 GPS (Global Positioning System), 304
 GRE (Generic Routing Encapsulation), 88, 410–411
 guest network, 289, 437–438
 GUI (graphical user interface), 415

H

half-duplex mode, 262
 hardware
 asset inventory, 327
 redundancy, 367–368, 370–372
 troubleshooting, 506–507, 522
 hashing algorithm, 345, 430–431
 header
 802.1Q, 268
 Flags field, 25

- IP (Internet Protocol), 23, 28, 57
- TCP (Transmission Control Protocol)
 - acknowledgment number, 24
 - sequence number, 24
 - window size, 24
- UDP (User Datagram Protocol), 25
- heat map, 102–103, 328–329
- HIDS (host-based intrusion detection system), 48–49
- high availability, 364
 - best practices, 369
 - design considerations, 368–369
 - measurement, 364
- HMAC (Hashed Message Authentication Code), 431
- hold-down timer, 239
- honeypot, 435–436
- hop count, 240
- hostname command, 562
- hosts file, 396–397
- hot site, 371
- hotspot, 286
- HSRP (Hot Standby Router Protocol), 248–249
- HTTP (Hypertext Transfer Protocol), 83
- HTTPS (Hypertext Transfer Protocol Secure), 84
- hub-and-spoke topology, 146–147
- hubs, 11
- humidity, 317–318
- hybrid cloud, 71, 72

- I
- IaaS (infrastructure as a service), 72
- IaC (infrastructure as code), 212–213
 - compliance, 214
 - configuration drift, 214
 - dynamic inventories, 215
 - playbook, 213
 - reusable tasks, 214
 - templates, 213–214
 - upgrades, 214
- IANA (Internet Assigned Numbers Authority), 174
- IBSS (independent basic service set), 286, 293–295
- ICANN (Internet Corporation for Assigned Names and Numbers), 174
- ICMP (Internet Control Message Protocol), 87, 467–468
- ICS (industrial control system), 437
- IDF (intermediate distribution frame), 279, 313
- IDS/IPS (intrusion detection system/intrusion prevention system), 46–47
 - anomaly-based, 48–49
 - policy-based, 48
 - signature-based, 48
- IEEE (Institute of Electrical and Electronics Engineers), 137
- ifconfig command, 553–554
- IGP (interior gateway protocol), 238
- IIoT (Industrial Internet of Things), 436
- IKE (Internet Key Exchange), 408–410
- IKEv2, 413
- incremental backup, 369
- index of refraction, 118
- infrastructure mode, 293
- initiator, 51
- inside global address, 245–246
- inside local address, 245–246
- integrity, 430–431
- intelligent PDU (power distribution unit), 316
- interface
 - graphical user, 415
 - media-dependent, 116
 - status, 518
 - troubleshooting, 505–506
- International Organization for Standardization (ISO), Open Systems Interconnection (OSI)

- model. *See* OSI (Open Systems Interconnection) model
 - Internet layer, TCP/IP stack, 23
 - IoT (Internet of Things), 136, 436, 481
 - IP (Internet Protocol) header, 23, 28, 57
 - IP address management
 - documentation, 328
 - tools, 334
 - ip command, 554
 - IP scanner, 546
 - IP spoofing, 463
 - IPAM (IP address management), 394
 - ipconfig command, 549–553
 - iperf, 545–546
 - IPsec, 408
 - AH (Authentication Header), 410–413
 - ESP (Encapsulating Security Payload), 410–413
 - IKE (Internet Key Exchange), 408–410
 - IKEv2, 413
 - tunnel, 409–410
 - IPsec (Internet Protocol Security), 89
 - IPv4, 170
 - address assignment, 175
 - address classes, 173–175
 - address structure, 171–172
 - addressing components, 175–176
 - APIPA (Automatic Private IP addressing), 180–181
 - CIDR (classless inter-domain routing), 196–197
 - dynamic configuration, 180
 - loopback address, 173
 - octet, 171
 - private addressing, 174
 - RFC1918 addresses, 174
 - static configuration, 176–180
 - subnet mask, 171–172, 175
 - subnetting, 181, 187–189
 - advanced, 192–196
 - borrowed bits, 185
 - calculating new IP address ranges, 189–192
 - calculating the number of available hosts, 186–187
 - calculating the number of created subnets, 185–186
 - extending a classful mask, 185
 - purpose, 182
 - subnet mask notation, 182–185
 - IPv6, 215
 - address structure, 217
 - address types, 217–218
 - data flows, 218–219
 - anycast, 220–221
 - multicast, 219
 - unicast, 219
 - need for, 216
 - packet types, 218
 - iSCSI (Internet Small Computer System Interface), 51
 - ISM bands, 102
 - isochronous transmission, 13
 - iterative lookup, 396
- ## J
- jitter, 56, 347, 531
 - jumbo frame, 51
 - jump box, 417
- ## K
- Kerberos, 440
 - key fob, 447
 - key management, 482
 - keylogger trojan, 468
 - Krone, 314
- ## L
- L2F (Layer 2 Forwarding), 414
 - L2TP (Layer 2 Tunneling Protocol), 414
 - LACP (Link Aggregation Control Protocol), 249–250, 276–277

LAN (local area network), 36, 137–138
 latency, 347, 531
 Layer 2 address, 12
 Layer 2 switch, 36–43
 LC (Lucent connector), 121
 LDAP (Lightweight Directory Access Protocol), 84, 440, 469
 LDAPS (Lightweight Directory Access Protocol over SSL), 85
 least privilege, 210, 433–434
 LED (light-emitting diode), 118, 504
 licensing asset inventory, 327
 life-cycle management, 329
 software management, 330–332
 vendor support announcements, 329–330
 lightweight AP, 53, 288–289
 link aggregation, 275–276
 link-state routing protocol, 242–245
 IS-IS (Intermediate System-to-Intermediate System), 242
 OSPF (Open Shortest Path First), 242, 250
 Linux, ip command, 554
 LLC (Logical Link Control) layer, data link sublayer, 13–14
 LLDP (Link Layer Discovery Protocol), 546–547
 load balancer, 49, 370
 local authentication, 417, 441
 lockable equipment rack, 315, 447
 logic bomb, 467
 logical diagram, 326
 logical segmentation, 436
 logical topology, 12, 143–144
 logs and logging
 aggregation, 354
 audit, 351
 Event Viewer, 353
 NetFlow, 354
 SIEM (security information and event management), 350

Syslog, 352–353
 traffic, 351
 loopback address, 173
 loopback plug, 508
 LSA (link-state advertisement), 242
 LTE (Long-Term Evolution), 108–109

M

MAC (media access control)
 address filtering, 301, 480
 address table corruption, 269
 data link sublayer, 12
 duplicate address, 520
 flooding, 462
 LLC (Logical Link Control) sublayer, 13–14
 malware, 463–465, 468
 MAN (metropolitan area network), 139
 management plane, SDN (software-defined networking), 206
 MD5 (Message Digest 5), 430
 MDF (main distribution frame), 314–315
 MDI (media-dependent interface), 116
 MDIX (media-dependent interface crossover), 116, 268, 505
 MDM (mobile device management), 438
 media. *See* cable
 media converter, 127
 memory
 buffering, 18–19
 monitoring, 347
 mesh topology, 295–296
 message/s
 DHCP, 386–387
 RA (Router Advertisement), 389
 SNMP, 343
 switching, 15
 Syslog, 352–353
 metered PDU (power distribution unit), 315
 metrics
 baseline, 347

- performance, 346–348
 routing protocol, 237, 238, 240
 MIB (management information base), 343
 microsegmentation, 36
 MIMO (multiple input, multiple output),
 107
 mini-GBIC, 126
 Miredo, 216
 MITRE Corporation, CVE (Common
 Vulnerabilities and Exposures)
 dictionary, 432
 MMF (multimode fiber), 118–120
 mnemonics, OSI (Open Systems
 Interconnection) model, 6
 mode of propagation, 118–119
 modulation, 8
 current state, 8
 state transition, 8
 monitoring. *See also* logs and logging
 availability, 356
 configuration, 357
 network, 342
 API integration, 354–355
 performance baselines, 519
 performance metrics/sensors,
 345–348
 SNMP, 342. *See also* SNMP (Simple
 Network Management Protocol)
 performance, 356
 routing table, 518
 SIEM (security information and event
 management), 443–444, 448
 motion detection, 444
 MPO (multi-fiber push on) connector,
 121
 MSTP (Multiple Spanning Tree
 Protocol), 274
 MTBF (mean time between failure), 364
 MTRJ (media termination recommended
 jack), 121
 MTTR (mean time to repair), 364
 MTU (maximum transmission unit), 11,
 263
 multicast transmission, 91–92, 219
 multifactor authentication, 417, 438–439,
 448
 multilayer switch, 43–45
 multimeter, 510
 multimode delay distortion, 120
 multipath issue, 297
 multiplexing, 10–11, 127
 multitenancy, 74
 MU-MIMO (multi-user MIMO), 107
- ## N
- NAC (network access control), 416, 435,
 480–481
 NACL (network access control list), 69
 name resolution, 390
 DNS (Domain Name System), 391
 dynamic, 394
 forward lookup zone, 395
 FQDN, 391–392
 global hierarchy, 392
 iterative lookup, 396
 over HTTPS, 396
 over TLS, 396
 primary zone, 395
 records, 393
 recursive lookup, 396
 reverse lookup zone, 396
 secondary zone, 395
 servers, 392
 TTL (Time-to-Live), 395
 zone transfer, 394
 NAS (network-attached storage), 51, 141
 NAT (network address translation), 175,
 244–246
 dynamic, 246
 gateway, 71
 static, 246
 NAT64, 216
 native VLAN, 267

- NDP (Neighbor Discovery Protocol), 263
- NetFlow, 354, 357, 546
- netstat command, 560–562
- network interface layer, TCP/IP stack, 23
- network layer, OSI model, 15–16
- network/s, 135. *See also* Ethernet; SDN (software-defined networking)
- access technologies, 414–417
- attached storage. *See* NAS (network-attached storage)
- in-band management, 418
- campus area. *See* CAN (campus area network)
- client/server, 140 -141
- cloud. *See* cloud/cloud computing
- collapsed core design, 152
- content delivery, 54
- converged, 52, 55, 137
- defining, 136
- design scenario, 373–374
- cost savings versus performance, 379
- environmental factors, 379
- IP addressing, 375–376
- Layer 1 media, 376
- Layer 2 devices, 376–377
- Layer 3 devices, 377–378
- topology, 374, 379–380
- wireless, 378
- diagram, 327
- discovery, 355
- fault tolerance, 365–366
- guest, 289, 437–438
- IDS/IPS (intrusion detection system / intrusion prevention system), 46–47
- anomaly-based, 48–49
- policy-based, 48
- signature-based, 46–47
- LAN (local area network). *See* LAN (local area network)
- layer settings, 518
- metropolitan area. *See* MAN (metropolitan area network)
- monitoring, 342
- API integration, 354–355
- performance metrics/sensors, 345–348
- SNMP, 342–345. *See also* SNMP (Simple Network Management Protocol)
- out-of-band management, 418
- peer-to-peer, 140, 141–143
- performance
- bandwidth, 530
- baselines, monitoring, 519
- bottlenecks, 530
- congestion/contention, 530
- jitter, 531
- latency, 531
- packet loss, 531
- troubleshooting, 523
- personal area. *See* PAN (personal area network)
- purpose, 136–137
- security group, 68–69
- security list, 69
- segmentation enforcement, 436
- sniffer, 349
- storage area, 51–52. *See also* SAN (storage area network)
- three-tier hierarchical model, 150
- access/edge layer, 150–151
- core layer, 152
- distribution/aggregation layer, 151–152
- topology, 143
- full-mesh, 147–148
- hub-and-spoke, 146–147
- hybrid, 150
- logical, 143–144
- partial-mesh, 148–150
- physical, 143
- point-to-point, 145

- spine and leaf, 153–154
star, 145–146
troubleshooting
 ACL settings, 521
 asymmetrical routing, 522
 blocked TCP/UDP ports, services, or addresses, 521
 BYOD challenges, 523
 collisions, 521
 DHCP scope exhaustion, 520
 duplicate IP address, 519
 duplicate MAC address, 520
 expired IP address, 520
 incorrect firewall settings, 521
 incorrect time, 520
 licensed feature issues, 523
 low optical link budget, 523
 missing routes, 522
 multicast flooding, 522
 rogue DHCP server, 520
 STP misconfiguration, 521
 switching loops, 522
virtual private. *See* VPN (virtual private network)
WAN (wide area network). *See* WAN (wide area network)
WLAN (wireless local area network).
 See WLAN (wireless local area network)
zones, 483
next-hop IP address, 235
NFC (Near Field Communication), 303
NFV (network functions virtualization), 66
NGFW (next-generation firewall), 57
NIC (network interface card), 14
 bonding, 367
 redundancy, 367–368
nmap command, 567
non-overlapping channels, 292
nonroot bridge, 272
north-south traffic flow, 155
NOS (network operating system), 141
notification, 348
nslookup command, 554–556
NTP (Network Time Protocol), 83, 398
NTS (Network Time Security), 399
- O**
- octet, 164, 171
OFDM (orthogonal frequency-division multiplexing), 10, 105
OFDMA (orthogonal frequency-division multiplexing), 11, 105
OID (object identifier), 343
omnidirectional antenna, 290–291
OpenVPN, 414
orchestration, 213
OS (operating system), update, 330–331
OSI (Open Systems Interconnection) model, 3, 4–5
application layer, 21–24
data link layer, 11–12
 LLC (Logical Link Control) sublayer, 13–14
 MAC sublayer, 12
mnemonics, 6
network layer, 15–16
PDU (protocol data unit), 6–7
physical layer, 7–11
presentation layer, 20–21
session layer, 19–20
transport layer, 17–18
OSPF (Open Shortest Path First), 242, 250
OT (operational technology), 437
OTDR (optical time-domain reflectometer), 508
out-of-band management, 418
outside global address, 245–246
outside local address, 245–246

P

- PaaS (platform as a service), 72
- packet/s
 - capture, 348–349, 465, 544–545
 - drops, 56, 506, 531
 - giant, 506
 - IPv6, 218
 - jitter, 56, 531
 - MTU (maximum transmission unit), 11
 - payload, 4
 - reordering, 16
 - runt, 506
 - switching, 15
- PAN (personal area network), 139
- parity bit, 14
- partial-mesh topology, 148–150
- password. *See also* authentication
 - attack, 462
 - spraying, 468
 - strong, 477
- PAT (port address translation), 246–248
- patch panel, 312, 313
- patching, 330, 477
- on-path attack, 459–460
- path-vector routing protocol, BGP
 - (Border Gateway Protocol), 243, 250
- payload, 4
- PCI DSS (Payment Card Industry Data Security Standards), 448
- PDU (protocol data unit), 6–7
- PDUs (power distribution units), 315–316, 319, 379
- peer-to-peer network, 140, 141–143
- penetration testing, 442
- performance
 - metrics, 346–348
 - monitoring, 356
 - network, 519, 523
 - bottlenecks, 530
 - congestion/contention, 530
- jitter, 531
- latency, 531
- packet loss, 531
- SLA (service-level agreement), 364
- PGP (Pretty Good Privacy), 428
- phishing, 464
- physical diagram, 326
- physical installation
 - environmental factors, 319
 - fire suppression, 318–319
 - humidity levels, 317–318
 - temperature, 317
- equipment rack, 314–315
- implications, 310–312
- locations, 313–314
- power, 315
 - load, 316
 - PDUs, 315–316
 - redundancy, 316
 - voltage, 316
- physical layer, OSI model, 7–11
- physical topology, 9, 143
- piggybacking, 464
- ping command, 547–549
- PKI (public key infrastructure), 429
- playbook, 213
- plenum cable, 117, 503
- PoE (Power over Ethernet), 277–278, 316, 507
- PoE+ (Power over Ethernet Plus), 278
- point-to-point topology, 145, 296
- poison reverse, 241
- polarity, antenna, 292
- policy
 - based authentication, 212–213
 - based authorization, 210
- CYOD (choose your own device), 438
- DLP (data loss prevention), 211
- regulatory compliance, 447–448
- separation of duties, 435
- policy-based IDS/IPS, 48
- port command, 466

- port/s, 86–87
- bonding, 276
- cost, 273
- DHCP (Dynamic Host Configuration Protocol), 83
- disabling, 478
- DNS (Domain Name System), 83
- FTP (File Transfer Protocol), 82
- HTTP (Hypertext Transfer Protocol), 83
- HTTPS (Hypertext Transfer Protocol Secure), 84
- LDAP (Lightweight Directory Access Protocol), 84
- LDAPS (Lightweight Directory Access Protocol over SSL), 85
- MDI/MDIX, 116
- mirroring, 348–350
- NTP (Network Time Protocol), 83
- numbers, 26–27
- RDP (Remote Desktop Protocol), 85
- scanner, 544–545
- security, 480
- SFTP (Secure File Transfer Protocol), 82
- SIP (Session Initiation Protocol), 85
- SMB (Server Message Block), 84
- SMTP (Simple Mail Transfer Protocol), 83
- SMTPS (Simple Mail Transfer Protocol Secure), 85
- SNMP (Simple Network Management Protocol), 84
- SQL server, 85
- SSH (Secure Shell), 82
- states, 274–275
- status, 506
- Syslog, 84
- tagging, 267
- Telnet, 82
- TFTP (Trivial File Transfer Protocol), 83
- troubleshooting, 504
- trunk, switch configuration, 268
- postmortem report, 495
- posture assessment, 442
- power
 - load, 316
 - PDUs (power distribution units), 315–316
 - redundancy, 316
 - uninterruptable, 317, 319
 - voltage, 316
- PPTP (Point-to-Point Tunneling Protocol), 414
- presentation layer, OSI model, 20–21
- primary zone, 395
- private cloud, 71, 72
- private VLAN, 479
- privilege escalation, 469
- process assessment, 443
- production configuration, 333
- programmable infrastructure, 213
- protocol/s. *See also* routing protocol/s;
 - time protocols
- analyzer, 544–545
- assigned ports, 82–85, 86–87
- connectionless, 27, 88
- connection-oriented, 88
- secure, 478
- VPN, 414
- provider, cloud, 68
- proxy server, 49–50
- PSK (pre-shred key), 301, 481
- PTP (Precision Time Protocol), 398
- public cloud, 71, 72
- punchdown block, 312
- punchdown tool, 508

Q-R

- QoS (quality of service), 55–57, 278
- RA (Router Advertisement) Guard, 479
- RA (Router Advertisement) message, 389
- rack diagram, 326

- rack size, 314
- RADIUS (Remote Authentication Dial-In User Service), 416, 439
- ransomware, 461
- RBAC (role-based access control), 434, 479–480
- RDP (Remote Desktop Protocol), 85
- records, DNS, 393
- recursive lookup, 396
- redundancy
 - hardware, 367–368, 370–372
 - NIC, 367–368
 - power, 316
- reference models, 4–5. *See also* OSI (Open Systems Interconnection) model; TCP/IP stack
- reflective attack, 458
- regulatory compliance, 447–448
- reliability, 364
- request process tracking, 332
- reverse lookup zone, 396
- reverse proxy server, 50
- RFC1918 addresses, 174
- RFI (radio frequency interference), 296, 297
- RG-6, 112
- RG-58, 112
- RG-59, 111
- ring topology, 143–144
- riser, 503
- risk, 433
 - assessment, 442
 - management, 441
- RJ11 connector, 116
- RJ45 connector, 116
- roaming, 297
- rogue AP, 461
- rogue DHCP server, 461
- root bridge, 271
- root bridge election, 272
- route command, 562–567
- routed protocol, 237
- routers and routing, 36. *See also* address translation
 - basic, 230–233
 - best match, 233
 - convergence, 236
 - directly connected routes, 233
 - dynamic routes, 235–237
 - Layer 3 to Layer 2 mapping, 233
 - loop prevention, 241
 - metrics, hop count, 240
 - next-hop IP address, 235
 - poison reverse, 241
 - routing table, 233
 - split horizon, 241
 - static routes, 234–235
 - wireless, 286–287
- routing protocol/s
 - AD (administrative distance), 237
 - advanced distance-vector, EIGRP, 242–243
 - characteristics, 237
 - distance vector, 239–241
 - dynamic, 243–244
 - exterior gateway, 238
 - hold-down timer, 239
 - interior gateway, 238
 - link-state, 242–245
 - IS-IS, 242
 - OSPF, 242, 250
 - metrics, 237, 238
 - path-vector, BGP, 243, 250
 - route redistribution, 244
- routing table
 - global, 436
 - monitoring, 518
- RPO (recovery point objective), 365
- RSA, 428–429
- RSTP (Rapid Spanning Tree Protocol), 269, 274
- RTO (recovery time objective), 365
- RTT (round-trip time), 17
- rules

firewall, 480
security, 482
runt, 506

S

SaaS (software as a service), 72
salami attack, 466
SAML (Security Assertion Markup Language), 441
SAN (storage area network), 51–52, 139
SASE (Secure Access Secure Edge), 211
satellite, 109–110
 delay, 110
 sensitivity to weather conditions, 110–111
SC (subscriber connector), 121
SCADA (supervisory control and data acquisition), 437
scalability, cloud, 75
scope, DHCP, 388
screened subnet, 435
SDN (software-defined networking), 205
 application plane, 205
 control plane, 207–208
 data plane, 206
 management plane, 206
SD-WAN (software-defined wide area network), 206–207, 221
 application awareness, 207
 central policy management, 208
 transport agnostic, 209–210
 zero-touch provisioning, 207
security. *See also* attack/s
 algorithm, 345
 CIA (confidentiality, integrity, and availability), 426
 availability, 431
 confidentiality, 426–430
 integrity, 430–431
 defense in depth, 434
 employee training, 445–446
 exploit, 433

least privilege, 433–434
level, 344–345
model, 344
physical, detection methods, 444–445
port, 480
prevention methods, 445–447
RBAC (role-based access control), 434
risk, 433
rules, 482
separation of duties, 435
threats, 432
vulnerability, 432
WLAN
 802.1X, 301–302
 disabling SSID broadcast, 301
 MAC address filtering, 301
 PSK (pre-shared key), 301
 rogue AP, 300
 war chalking, 299
 war dialing, 299
 war driving, 299
 WPA cracking, 300
 WPA2, 303
 WPA3, 303
 zero trust, 211
segmentation
 enforcement, 436
 logical, 436
 VLAN, 478
Seifert, Rich, *The Switch Book*, 5
separation of duties, 435
sequence number field, 24
server/s
 cluster, 368
 commercial off-the-shelf, 66
 DHCP, 388–389
 DNS (Domain Name System), 392
 multitenancy, 74
 NTP (Network Time Protocol), 398
 proxy, 49–50
 reverse proxy, 50
 rogue, 461

- screened subnet, 435
- SQL, ports, 85
- Syslog, 351
- TFTP, 546
- service/s
 - advertisement, 21
 - request, 332
- session hijacking, 466
- session layer, OSI model, 19–20
- SFTP (Secure File Transfer Protocol), 82
- SHA (Secure Hash Algorithm), 431
- shared bus topology, 258
- short, 504
- shoulder surfing, 464
- show commands, 567–568
- SIEM (security information and event management), 350, 357, 441, 443–444, 448
- signature-based IDS/IPS, 48
- single point of failure, 365–366
- SIP (Session Initiation Protocol), 85
- site survey, 534
- site-to-site VPN, 406–407
- skimming, 468
- SLA (service-level agreement), 328, 364
- SLAAC (stateless address autoconfiguration), 389–390
- sliding window, 17–18
- smart card, 446
- smart locker, 447
- SMB (Server Message Block), 84
- SMF (single-mode fiber), 118, 120
- SMTP (Simple Mail Transfer Protocol), 83
- SMTSP (Simple Mail Transfer Protocol Secure), 85
- snapshot, 369
- SNAT (Static NAT), 246
- snips/cutters, 511
- SNMP (Simple Network Management Protocol), 84
 - community strings, 343
- messages, 343
- MIB (management information base), 343
- OID (object identifier), 343
- security level, 344–345
- version 3, 344–347
- social engineering attacks, 463–464
 - dumpster diving, 464
 - phishing, 464
 - piggybacking, 464
 - shoulder surfing, 464
 - tailgating, 464
- software
 - command and control, 459
 - management, 330–332, 459
 - bug fix, 330
 - firmware update, 331
 - OS update, 330–331
 - patching, 330
- software asset inventory, 327
- source control systems, 215–217
- SP (service provider), 155
- SPB (Shortest Path Bridging), 269
- spectrum analyzer, 511
- spine and leaf topology, 153–154
- split horizon, 241
- split tunnel VPN, 407
- Splunk Enterprise, 357
- spoofing
 - ARP, 459, 461
 - DNS, 460
 - IP, 463
 - MAC, 462
- SQL (Structured Query Language)
 - injection attack, 468
 - server, ports, 85
- SSE (Security Service Edge), 211–212
- SSH (Secure Shell), 27, 82, 415
- SSID (service set identifier), 300
- SSL (Secure Sockets Layer), 414
- SSO (single sign-on), 439

- SSTP (Secure Socket Tunneling Protocol), 414
- ST (straight tip) connector, 120
- standards
- cable, TIA/EIA-568, 113
 - WLAN, 108
 - 802.11a, 106
 - 802.11ac, 107
 - 802.11ax, 107–108
 - 802.11b, 106
 - 802.11g, 106
 - 802.11n, 106–107
 - star topology, 145–146
 - state transition modulation, 8
 - stateful firewall, 45
 - static configuration, IPv4, 176–180
 - static routes, 234–235
 - StatTDM (statistical time-division multiplexing), 10
 - storage, network-attached, 51
 - STP (shielded twisted-pair) cable, 113–114
 - STP (Spanning Tree Protocol), 269, 271, 271, 279, 478
 - BPDU (bridge protocol data unit), 273
 - identifying port roles, 273
 - misconfiguration, 521
 - modern enhancements, 274
 - nonroot bridge, 272
 - port
 - cost, 273
 - states, 274–275
 - root bridge election, 272
 - straight-through cable, 115
 - stratum, 398
 - structured troubleshooting methodology
 - establish a theory of probable cause, 493
 - identify the problem, 493
 - implement the solution or escalate, 494
 - postmortem report, 495
 - resolve the problem and identify potential effects, 494
 - test the theory to determine the cause, 493
 - verify full system functionality, 494
 - subinterface, 250. *See also* interface
 - subnet mask, 171–172, 175
 - subnetting, 181, 187–189
 - advanced, 192–196
 - borrowed bits, 185
 - calculating new IP address ranges, 189–192
 - calculating the number of available hosts, 186–187
 - calculating the number of created subnets, 185–186
 - extending a classful mask, 185
 - purpose, 182
 - subnet mask notation, 182–185
 - supply chain attack, 468
 - surveillance camera, 444
 - SVI (switch virtual interface), 264
 - switches and switching, 15. *See also* Ethernet; port/s; VLAN (virtual LAN)
 - access port configuration, 266–267
 - broadcast storm, 270–271
 - circuit, 15
 - configuration for a trunk port, 268
 - content, 370–371
 - Layer 2, 36–43
 - link aggregation, 275–277
 - loops, 522. *See also* STP (Spanning Tree Protocol)
 - MAC address table corruption, 269
 - message, 15
 - multilayer, 43–45
 - packet, 15
 - PoE (Power over Ethernet), 277–278
 - switchport port-security command, 266–267
 - symmetric encryption, 427–428

- synchronization
 - asynchronous transmission, 13
 - bit, 9
 - isochronous transmission, 13
 - synchronous transmission, 14
 - synchronous transmission, 14
- Syslog, 84, 352–353
 - clients, 352
 - message, 352–353
 - server, 351
 - severity levels, 352
- T**
 - tabletop exercise, 372
 - TACACS+ (Terminal Access Controller Access-Control System), 416, 439
 - tailgating, 464
 - tamper detection, 445
 - tap, 569
 - TCP (Transmission Control Protocol),
 - 17, 88
 - header
 - acknowledgment number, 24
 - Flags field, 25
 - sequence number, 24
 - window size, 24
 - SYN flood, 467
 - windowing, 17–18
 - tcpdump command, 567
 - TCP/IP stack, 22
 - application layer, 25
 - application protocols, 26–27
 - Internet layer, 23
 - IP protocol types, 87–90
 - network interface layer, 23
 - transport layer, 24–25
 - TDM (time-division multiplexing), 10
 - TDR (time-domain reflectometer), 508
 - technology-based attacks
 - ARP poisoning, 460
 - ARP spoofing, 461
 - DDoS (distributed denial-of-service),
 - 459
 - deauthentication, 463
 - DNS poisoning, 460
 - DoS (denial-of-service), 458–459
 - evil twin, 461
 - IP spoofing, 463
 - MAC flooding, 462
 - MAC spoofing, 462
 - malware, 463–465
 - password, 462
 - on-path, 459–460
 - ransomware, 461
 - rogue access point, 461
 - rogue DHCP servers, 461
 - VLAN hopping, 460
- Telnet, 82
- telnet command, 567
- temperature control, 317, 346
- template, IaC (infrastructure as code),
 - 213–214
- Teredo tunneling, 216
- test/ing
 - disaster recovery, 372–373
 - penetration, 442
 - validation, 372
- tethering, 109
- text, formatting, 20
- TFA (two-factor authentication), 417
- TFTP (Trivial File Transfer Protocol),
 - 83, 546
- threat/s, 432
 - advanced persistent, 468
 - assessment, 442
- three-tier hierarchical model, 150
 - access/edge layer, 150–151
 - core layer, 152
 - distribution/aggregation layer, 151–152
- throughput, 531
- TIA/EIA-568 standard, 113
- time protocols, 397

- NTP (Network Time Protocol), 397–398
NTS (Network Time Security), 399
PTP (Precision Time Protocol), 398
time-based authentication, 441
TLS (Transport Layer Security), 414
tone generator, 569
tools
 cable tester, 569
 command-line
 arp, 558–560
 dig, 556–557
 hostname, 562
 ifconfig, 553–554
 ip, 554
 ipconfig, 549–553
 netstat, 560–562
 nmap, 567
 nslookup, 554–556
 ping, 547–549
 route, 562–567
 show, 567–568
 tcpdump, 567
 telnet, 567
 traceroute, 557–558
CompTIA Network+ N10-009 exam
 preparation, 577–578
IP address management, 334
network sniffer, 349
packet capture, 348–349
tap, 569
tone generator, 569
troubleshooting, 507, 544–545
 bandwidth speed tester, 544
 cable crimper, 507
 cable stripper, 511
CDP (Cisco Discovery Protocol), 547
 fiber light meter, 511
 fusion splicer, 511
IP scanner, 546
iperf, 545–546

LLDP (Link Layer Discovery Protocol), 546–547
loopback plug, 508
multimeter, 510
NetFlow analyzer, 546
OTDR (optical time-domain reflectometer), 508
port scanner, 544–545
punchdown tool, 508
snips/cutters, 511
spectrum analyzer, 511
TDR (time-domain reflectometer), 508
TFTP server, 546
 wire map tester, 510
visual fault locator, 569
Wi-Fi analyzer, 569
topology, 143, 374. *See also* network/s
 full-mesh, 147–148
 hub-and-spoke, 146–147
 hybrid, 150
 logical, 12, 143–144
 mesh, 295–296
 partial-mesh, 148–150
 physical, 9, 143
 point-to-point, 145, 296
 ring, 143–144
 shared bus, 258
 spine and leaf, 153–154
 star, 145–146
traceroute command, 557–558
traffic, 93–94
 analysis, 356
 anycast, 92–93
 broadcast, 91
 east-west flows, 155
 logs, 351
 multicast, 91–92
 north-south flows, 155
 unicast, 90
training, employee, 445–446
transceiver, 126–127, 507

- transport agnostic, 209–210
- transport layer
 - OSI model, 17–18
 - TCP/IP stack, 24–25
- troubleshooting
 - cable issues, 531–533
 - connectivity, 490
 - diagnosing the problem, 490, 491
 - hardware, 506–507, 522
 - interface issues, 505–506
 - network
 - ACL settings, 521
 - asymmetrical routing, 522
 - blocked TCP/UDP ports, services, or addresses, 521
 - BYOD challenges, 523
 - collisions, 521
 - DHCP scope exhaustion, 520
 - duplicate IP address, 519
 - duplicate MAC address, 520
 - expired IP address, 520
 - incorrect firewall settings, 521
 - incorrect time, 520
 - licensed feature issues, 523
 - low optical link budget, 523
 - missing routes, 522
 - multicast flooding, 522
 - performance, 523
 - rogue DHCP server, 520
 - STP misconfiguration, 521
 - switching loops, 522
 - port, 504
 - resolving the problem, 490
 - structured methodology, 492–493
 - establish a theory of probable cause, 493
 - identify the problem, 493
 - implement the solution or escalate, 494
 - postmortem report, 495
 - resolve the problem and identify potential effects, 494
 - test the theory to determine the cause, 493
 - verify full system functionality, 494
 - tools, 507. *See also* command/s
 - bandwidth speed tester, 544
 - cable crimper, 507
 - cable stripper, 511
 - CDP (Cisco Discovery Protocol), 547
 - fiber light meter, 511
 - fusion splicer, 511
 - IP scanner, 546
 - iperf, 545–546
 - LLDP (Link Layer Discovery Protocol), 546–547
 - loopback plug, 508
 - multimeter, 510
 - NetFlow analyzer, 546
 - OTDR (optical time-domain reflectometer), 508
 - port scanner, 544–545
 - protocol analyzer/packet capture, 544–545
 - punchdown tool, 508
 - snips/cutters, 511
 - spectrum analyzer, 511
 - TDR (time-domain reflectometer), 508
 - TFTP server, 546
 - wire map tester, 510
 - wireless/WLAN, 536–537
 - antenna, 533
 - common issues, 534–536
 - frequencies and channels, 533–534
 - performance issues, 531–533
 - trunking, 267–268
 - trust relationship exploitation, 467
 - TTL (Time-to-Live) field, 23
 - tunnel
 - child, 413
 - GRE (Generic Routing Encapsulation), 410–411

IPsec, 409–410
VPN, 407
twinax, 112, 113
twisted pair cable
connectors, 116–117
shielded, 113–114
unshielded, 114–116

U

UDP (User Datagram Protocol), 17, 25, 27, 88
unicast transmission, 90, 219
unidirectional antenna, 291
update
device, 477
firmware, 331
operating system, 330–331
upgrade, firmware, 477
UPS (uninterruptable power supply), 317, 319
URL (uniform resource locator), 394
USB drop attack, 468
UTP (unshielded twisted pair) cable, 114–116

V

validation test, 372
vendor
assessment, 443
support announcements, 329–330
virtual desktop, 415
virtualization, NFV (network functions virtualization), 66
visual fault locator, 569
VLAN (virtual LAN), 263–265, 279
assignment, 519
default, 479
hopping, 460
native, 267
private, 479
segmentation, 478

trunking, 267–268
voice, 265
VLSM (Variable-Length Subnet Mask), 182
VM (virtual machine), 154
voice VLAN, 265
voltage, 316
VPC (virtual private cloud), 67–68
VPN (virtual private network), 55, 73, 406, 414
clientless, 407
client-to-site, 406
full tunnel, 407
IPsec, 408
AH, 410–413
ESP, 410–413
IKE, 408–410
IKEv2, 413
tunnel, 409–410
site-to-site, 406–407
split tunnel, 407
tunnel, 407
VRRP (Virtual Router Redundancy Protocol), 249
VTEP (Virtual Tunnel Endpoint), 209
VTP (VLAN Trunking Protocol), 265
vulnerability, 432, 442
VXLAN (virtual extensible local area network), 208
DCI (data center interconnect), 209
Layer 2 encapsulation, 208–209
VTEP (Virtual Tunnel Endpoint), 209

W

WAN (wide area network), 138
war chalking, 299
war dialing, 299
war driving, 299
warm site, 371
warranty support asset inventory, 327
WDM (bidirectional wavelength-division multiplexing), 127

- Wi-Fi 5, 107
- Wi-Fi 6, 107–108
- Wi-Fi analyzer, 569
- windowing, 17–18
- Windows
 - Event Viewer, 353
 - IPv4, static configuration, 176–180
- WINS (Windows Internet Name Service), 175
- wire map tester, 510
- wireless/WLAN, 138, 286. *See also* AP (access point)
 - 2.4GHz band, 102–104
 - 5GHz band, 104
 - ad hoc, 286, 293
 - antenna, 289–290
 - gain, 290
 - omnidirectional, 290–291
 - polarity, 292
 - unidirectional, 291
 - AP (access point), 52–53, 287–289
 - autonomous, 288
 - lightweight, 288–289
 - placement, 296–301
 - captive portal, 289
 - cell, 297
 - channel/s, 102–103
 - center frequency, 105
 - non-overlapping, 292
 - width, 292
 - client isolation, 481
 - devices, 296
 - DSSS (direct-sequence spread spectrum), 105
 - EIRP (effective isotropic radiated power), 532
 - ESS (extended service set), 295
 - FHSS (frequency-hopping spread spectrum), 105
 - frequency bands, 102
 - guest network, 289
- hotspot, 286
- IBSS (independent basic service set), 286, 293–295
- infrastructure mode, 293
- ISM bands, 102
- mesh topology, 295–296
- multipath issue, 297
- OFDM (orthogonal frequency-division multiplexing), 105
- OFDMA (orthogonal frequency-division multiplexing), 105
- RFI (radio frequency interference), 296, 297
- rogue AP, 300
- RSSI (received signal strength indication), 532
- security, 299
 - 802.1X, 301–302
 - disabling SSID broadcast, 301
 - MAC address filtering, 301
 - PSK (pre-shared key), 301
 - war chalking, 299
 - war dialing, 299
 - war driving, 299
 - WPA cracking, 300
 - WPA2, 303
 - WPA3, 303
 - signal strength, 297
 - site survey, 534
 - standards. *See* standards, WLAN survey, 328–329
 - troubleshooting, 536–537
 - antenna, 533
 - common issues, 534–536
 - frequencies and channels, 533–534
 - performance, 531–533
 - wireless routers, 286–287
 - wiretapping, 465
 - wiring closet, 312
 - WLC (wireless LAN controller), 53

WPA (Wi-Fi Protected Access), security cracking, 300
WPA2, 303
WPA3, 303

X-Y-Z

zero-day attack, 432
zero-touch provisioning, 207

zombie, 459
zone transfer, 394
zones, 483
ZTA (zero-trust architecture), 209, 221–222
least privilege access, 210
policy-based authentication, 212–213
policy-based authorization, 210