

PEARSON IT
CERTIFICATION

Save 10%
on Exam
Voucher

See Inside

 Practice
Tests

 Video
Training

 Flash
Cards

 Review
Exercises

 Labs

 Interactive
Study Guide

 Study
Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Network+

N10-008



ANTHONY SEQUEIRA
CCIE® NO.15626

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



CompTIA[®] Network+ N10-008 Cert Guide

Anthony Sequeira, CCIE No. 15626
Pearson IT Certification



CompTIA® Network+ N10-008 Cert Guide

Anthony Sequeira

Copyright © 2022 Pearson IT Certification

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

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

ISBN-13: 978-0-13-744994-1

ISBN-10: 0-13-744994-1

Library of Congress Control Number: 2021911389

ScoutAutomatedPrintCode

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 screen shots may be viewed in full within the software version specified.

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

Editor-in-Chief

Mark Taub

Director, ITP Product Management

Brett Bartow

Managing Editor

Sandra Schroeder

Development Editor

Christopher Cleveland

Project Editor

Mandie Frank

Copy Editor

Kitty Wilson

Technical Editor

Chris Crayton

Editorial Assistant

Cindy Teeters

Designer

Chuti Prasertsith

Composition

codeMantra

Indexer

Ken Johnson

Proofreader

Charlotte Kughen

Warning and Disclaimer

This book is designed to provide information about IT networking in the scope of the CompTIA Network+ exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Pearson.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Figure	Attribution
Figure 2-1	Courtesy of Cisco Systems, Inc
Figure 2-2	Courtesy of Cisco Systems, Inc
Figure 2-3	Courtesy of Cisco Systems, Inc
Figure 2-4	Courtesy of Cisco Systems, Inc
Figure 2-5	Courtesy of Cisco Systems, Inc
Figure 2-6	Courtesy of Cisco Systems, Inc
Figure 2-7	Courtesy of Cisco Systems, Inc
Figure 2-8	Courtesy of Cisco Systems, Inc
Figure 2-10	Courtesy of Cisco Systems, Inc
Figure 2-11	Courtesy of Cisco Systems, Inc
Figure 2-12	Courtesy of Cisco Systems, Inc
Figure 2-13	Courtesy of Cisco Systems, Inc
Figure 2-14	Courtesy of Cisco Systems, Inc
Figure 2-15	Courtesy of Cisco Systems, Inc
Figure 2-16	Screenshot of Configuring a vNIC © 2021, Oracle and/or its affiliates
Figure 2-17	Courtesy of Cisco Systems, Inc
Figure 2-18	Screenshot of Configuring a Virtual Switch © Microsoft 2021
Figure 2-19	Courtesy of Cisco Systems, Inc
Figure 2-20	Courtesy of Cisco Systems, Inc
Figure 2-21	Courtesy of Cisco Systems, Inc
Figure 2-22	Courtesy of Cisco Systems, Inc
Figure 2-23	Courtesy of Cisco Systems, Inc
Figure 4-4	Courtesy of Cisco Systems, Inc
Figure 4-5	Courtesy of Cisco Systems, Inc
Figure 4-6	Courtesy of Cisco Systems, Inc
Figure 4-7	Screenshot of Windows Control Panel © Microsoft 2021
Figure 4-8	Screenshot of Network and Internet Control Panel © Microsoft 2021
Figure 4-9	Screenshot of Network and Sharing Center © Microsoft 2021
Figure 4-10	Screenshot of Network Connections Window © Microsoft 2021
Figure 4-11	Screenshot of Local Area Connection Status Window © Microsoft 2021
Figure 4-12	Screenshot of Local Area Connection Properties © Microsoft 2021
Figure 4-13	Screenshot of Internet Protocol Version 4 (TCP/IPv4) Properties © Microsoft 2021

Figure 4-14	Screenshot of Advanced TCP/IP Settings: DNS Tab © Microsoft 2021
Figure 4-15	Screenshot of Advanced TCP/IP Settings: WINS Tab © Microsoft 2021
Figure 4-16; Figure 6-2	Screenshot of Configuring Microsoft Windows 10 to Obtain IP Address Information via DHCP © Microsoft 2021
Figure 4-17	Screenshot of APIPA Configuration Enabled by Default © Microsoft 2021
Figure 4-18	Courtesy of Cisco Systems, Inc
Figure 4-19	Screenshot of Free IP Address Manager © 2021 SolarWinds Worldwide, LLC
Figure 4-21	Courtesy of Cisco Systems, Inc
Figure 4-22	Courtesy of Cisco Systems, Inc
Figure 4-23	Courtesy of Cisco Systems, Inc
Figure 4-24	Courtesy of Cisco Systems, Inc
Figure 4-25	Courtesy of Cisco Systems, Inc
Figure 6-1	Courtesy of Cisco Systems, Inc
Figure 6-3	Courtesy of Cisco Systems, Inc
Figure 9-1	Courtesy of Cisco Systems, Inc
Figure 9-2	Courtesy of Cisco Systems, Inc
Figure 9-3	Courtesy of Cisco Systems, Inc
Figure 9-4	Courtesy of Cisco Systems, Inc
Figure 9-5	Courtesy of Cisco Systems, Inc
Figure 9-6	Courtesy of Cisco Systems, Inc
Figure 9-7	Courtesy of Cisco Systems, Inc
Figure 9-8	Courtesy of Cisco Systems, Inc
Figure 9-9	Courtesy of Cisco Systems, Inc
Figure 9-10	Courtesy of Cisco Systems, Inc
Figure 9-11	Courtesy of Cisco Systems, Inc
Figure 9-12	Courtesy of Cisco Systems, Inc
Figure 9-13	Courtesy of Cisco Systems, Inc
Figure 9-14	Courtesy of Cisco Systems, Inc
Figure 9-15	Courtesy of Cisco Systems, Inc
Figure 9-16	Courtesy of Cisco Systems, Inc
Figure 9-17	Norman Chan/Shutterstock
Figure 9-18	Courtesy of Cisco Systems, Inc
Figure 9-19	Courtesy of Cisco Systems, Inc
Figure 9-20	Courtesy of Cisco Systems, Inc
Figure 9-21	Courtesy of Cisco Systems, Inc
Figure 9-22	Courtesy of Cisco Systems, Inc
Figure 10-1	Courtesy of Cisco Systems, Inc
Figure 10-2	Courtesy of Cisco Systems, Inc

Figure 10-3	Courtesy of Cisco Systems, Inc
Figure 10-4	Courtesy of Cisco Systems, Inc
Figure 10-5	Courtesy of Cisco Systems, Inc
Figure 10-6	Courtesy of Cisco Systems, Inc
Figure 10-7	Courtesy of Cisco Systems, Inc
Figure 10-8	Courtesy of Cisco Systems, Inc
Figure 10-9	Courtesy of Cisco Systems, Inc
Figure 10-10	Courtesy of Cisco Systems, Inc
Figure 10-11	Courtesy of Cisco Systems, Inc
Figure 10-12	Courtesy of Cisco Systems, Inc
Figure 10-13	Courtesy of Cisco Systems, Inc
Figure 11-4	Courtesy of Cisco Systems, Inc
Figure 11-7	Courtesy of Cisco Systems, Inc
Figure 11-8	Courtesy of Cisco Systems, Inc
Figure 11-9	Courtesy of Cisco Systems, Inc
Figure 11-10	Courtesy of Cisco Systems, Inc
Figure 11-11	Courtesy of Cisco Systems, Inc
Figure 11-13	Courtesy of Cisco Systems, Inc
Figure 11-14	Courtesy of Cisco Systems, Inc
Figure 11-15	Courtesy of Cisco Systems, Inc
Figure 11-16	Courtesy of Cisco Systems, Inc
Figure 11-17	Courtesy of Cisco Systems, Inc
Figure 11-18	Courtesy of Cisco Systems, Inc
Figure 11-19	Courtesy of Cisco Systems, Inc
Figure 11-20	Courtesy of Cisco Systems, Inc
Figure 11-21	Screenshot of Example: Wireshark Packet-Capture Software © Wireshark Foundation
Figure 11-22	Courtesy of Cisco Systems, Inc
Figure 11-23	Courtesy of Cisco Systems, Inc
Figure 11-24	Courtesy of Cisco Systems, Inc
Figure 11-25	Courtesy of Cisco Systems, Inc
Figure 12-1	Courtesy of Cisco Systems, Inc
Figure 12-2	Courtesy of Cisco Systems, Inc
Figure 12-3	Courtesy of Cisco Systems, Inc
Figure 12-4	Courtesy of Cisco Systems, Inc
Figure 12-6	Courtesy of Cisco Systems, Inc
Figure 12-7	Courtesy of Cisco Systems, Inc
Figure 12-8	Courtesy of Cisco Systems, Inc
Figure 12-12	Courtesy of Cisco Systems, Inc
Figure 13-1	Courtesy of Cisco Systems, Inc
Figure 13-2	Courtesy of Cisco Systems, Inc
Figure 13-3	Courtesy of Cisco Systems, Inc

Figure 13-4	Screenshot of Structure of a Syslog Message © 2021 SolarWinds Worldwide, LLC
Figure 13-5	Screenshot of Application Log © Microsoft 2021
Figure 13-6	Screenshot of Security Log © Microsoft 2021
Figure 13-7	Screenshot of System Log © Microsoft 2021
Figure 15-1	Courtesy of Cisco Systems, Inc
Figure 15-2	Courtesy of Cisco Systems, Inc
Figure 15-3	Courtesy of Cisco Systems, Inc
Figure 15-4	Courtesy of Cisco Systems, Inc
Figure 15-5	Courtesy of Cisco Systems, Inc
Figure 15-6	Courtesy of Cisco Systems, Inc
Figure 15-8	Courtesy of Cisco Systems, Inc
Figure 16-1	Courtesy of Cisco Systems, Inc
Figure 16-2	Courtesy of Cisco Systems, Inc
Figure 17-1	Courtesy of Cisco Systems, Inc
Figure 19-1	Courtesy of Cisco Systems, Inc
Figure 19-2	Courtesy of Cisco Systems, Inc
Figure 19-4	Courtesy of Cisco Systems, Inc
Figure 23-1	Screenshot of Wireshark Protocol Analyzer Software © Wireshark Foundation
Figure 24-1	Courtesy of Cisco Systems, Inc
UNPHCov-1	leo_photo/Shutterstock
Cover Credit	TippaPatt/Shutterstock

Contents at a Glance

Introduction xxxviii

Part I: Networking Fundamentals

- CHAPTER 1 The OSI Model and Encapsulation 3
- CHAPTER 2 Network Topologies and Types 35
- CHAPTER 3 Network Media Types 79
- CHAPTER 4 IP Addressing 105
- CHAPTER 5 Common Ports and Protocols 165
- CHAPTER 6 Network Services 181
- CHAPTER 7 Corporate and Datacenter Architectures 197
- CHAPTER 8 Cloud Concepts 211

Part II: Network Implementations

- CHAPTER 9 Various Network Devices 221
- CHAPTER 10 Routing Technologies and Bandwidth Management 255
- CHAPTER 11 Ethernet Switching 283
- CHAPTER 12 Wireless Standards 321

Part III: Network Operations

- CHAPTER 13 Ensure Network Availability 353
- CHAPTER 14 Organizational Documents and Policies 375
- CHAPTER 15 High Availability and Disaster Recovery 393

Part IV: Network Security

- CHAPTER 16 Common Security Concepts 417
- CHAPTER 17 Common Types of Attacks 439
- CHAPTER 18 Network Hardening Techniques 453
- CHAPTER 19 Remote Access Methods 465
- CHAPTER 20 Physical Security 485

Part V: Network Troubleshooting

- CHAPTER 21** A Network Troubleshooting Methodology 495
- CHAPTER 22** Troubleshoot Common Cabling Problems 505
- CHAPTER 23** Network Software Tools and Commands 519
- CHAPTER 24** Troubleshoot Common Wireless Issues 549
- CHAPTER 25** Troubleshoot General Network Issues 561

Part VI: Final Preparation

- CHAPTER 26** Final Preparation 571

Glossary of Key Terms 579

- APPENDIX A** Answers to Review Questions 623

- APPENDIX B** CompTIA Network+ (N10-008) Cert Guide Exam Updates 639
- Index 641

ONLINE ELEMENTS:

APPENDIX C Memory Tables

APPENDIX D Memory Tables Answer Key

APPENDIX E Study Planner

Exam Essentials Interactive Study Guide

Key Terms Flash Cards Application

Instructional Videos

Performance-Based Exercises

CompTIA Network+ N10-008 Hands-On Lab Simulator Lite Software

Table of Contents

Introduction xxxviii

Part I: Networking Fundamentals

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 15

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

Complete Chapter 1 Hands-On Labs in Network+ Simulator Lite 30

Additional Resources 30

Review Questions 30

Chapter 2 Network Topologies and Types 35

Foundation Topics 36

Defining a Network 36

The Purpose of Networks 36

Network Types and Characteristics	37
LAN	37
WAN	38
WLAN	38
SAN	38
Other Categories of Networks	39
<i>CAN</i>	39
<i>MAN</i>	39
<i>PAN</i>	39
<i>Software-Defined Wide Area Network (SD-WAN)</i>	39
<i>Multiprotocol Label Switching</i>	40
<i>Multipoint Generic Routing Encapsulation (mGRE)</i>	41
Networks Defined Based on Resource Location	42
Client/Server Networks	42
Peer-to-Peer Networks	43
Networks Defined by Topology	45
Physical Versus Logical Topology	45
Bus Topology	46
Ring Topology	48
Star Topology	50
Hub-and-Spoke Topology	51
Full-Mesh Topology	52
Partial-Mesh Topology	53
Service-Related Entry Points	55
Virtual Network Concepts	55
Virtual Servers	55
Virtual Routers and Firewalls	58
Virtual Switches (vSwitches)	58
Virtual Desktops	58
Other Virtualization Solutions	60
Provider Links	60
Satellite	60
Digital Subscriber Line	62

	Cable Modem	64
	Leased Line	65
	T1	66
	E1	66
	T3	67
	E3	67
	Metro-optical	67
	Synchronous Optical Network	67
	Real-World Case Study	69
	Summary	69
	Exam Preparation Tasks	70
	Review All the Key Topics	70
	Complete Tables and Lists from Memory	71
	Define Key Terms	71
	Additional Resources	71
	Review Questions	72
Chapter 3	Network Media Types	79
	Foundation Topics	80
	Copper and Fiber Media and Connectors	80
	Coaxial Cable	80
	Twisted-Pair Cable	82
	<i>Shielded Twisted Pair</i>	82
	<i>Unshielded Twisted Pair</i>	83
	<i>Twisted-Pair Cable Connectors</i>	85
	Plenum Versus Nonplenum Cable	86
	Fiber-Optic Cable	86
	<i>Multimode Fiber</i>	87
	<i>Single-Mode Fiber</i>	89
	<i>Fiber-Optic Cable Connectors</i>	89
	<i>Fiber Connector Polishing Styles</i>	90
	Ethernet and Fiber Standards	90
	Distance and Speed Limitations	93
	Transceivers	95

	Multiplexing in Fiber-Optic Networks	95
	Cable Management	96
	Media Converters	99
	Real-World Case Study	99
	Summary	99
	Exam Preparation Tasks	100
	Review All the Key Topics	100
	Complete Tables and Lists from Memory	100
	Define Key Terms	100
	Additional Resources	101
	Review Questions	101
Chapter 4	IP Addressing	105
	Foundation Topics	106
	Binary Numbering	106
	Principles of Binary Numbering	106
	Converting a Binary Number to a Decimal Number	107
	Converting a Decimal Number to a Binary Number	107
	Binary Numbering Practice	109
	Binary Conversion Exercise 1	109
	Binary Conversion Exercise 1: Solution	109
	Binary Conversion Exercise 2	110
	Binary Conversion Exercise 2: Solution	110
	Binary Conversion Exercise 3	110
	Binary Conversion Exercise 3: Solution	111
	Binary Conversion Exercise 4	111
	Binary Conversion Exercise 4: Solution	112
	IPv4 Addressing	112
	IPv4 Address Structure	113
	Classes of Addresses	114
	Types of Addresses	116
	<i>Unicast</i>	117
	<i>Broadcast</i>	117
	<i>Multicast</i>	118

Assigning IPv4 Addresses	118
IP Addressing Components	119
Static Configuration	120
Dynamic Configuration	126
BOOTP	126
DHCP	126
Automatic Private IP Addressing	128
Subnetting	129
Purpose of Subnetting	129
Subnet Mask Notation	130
Subnet Notation: Practice Exercise 1	132
Subnet Notation: Practice Exercise 1 Solution	132
Subnet Notation: Practice Exercise 2	132
Subnet Notation: Practice Exercise 2 Solution	132
Extending a Classful Mask	132
Borrowed Bits	133
Calculating the Number of Created Subnets	133
Calculating the Number of Available Hosts	134
Basic Subnetting Practice: Exercise 1	134
Basic Subnetting Practice: Exercise 1 Solution	135
Basic Subnetting Practice: Exercise 2	136
Basic Subnetting Practice: Exercise 2 Solution	136
Calculating New IP Address Ranges	137
Advanced Subnetting Practice: Exercise 1	139
Advanced Subnetting Practice: Exercise 1 Solution	139
Advanced Subnetting Practice: Exercise 2	140
Advanced Subnetting Practice: Exercise 2 Solution	141
Additional Practice	143
Classless Interdomain Routing	144
Address Translation	145
NAT	145
PAT	147
IP Version 6	149
Need for IPv6	149

IPv6 Address Structure	150
IPv6 Address Types	150
IPv6 Data Flows	151
<i>Unicast</i>	152
<i>Multicast</i>	152
<i>Anycast</i>	153
Real-World Case Study	154
Summary	154
Exam Preparation Tasks	155
Review All the Key Topics	155
Complete Tables and Lists from Memory	156
Define Key Terms	156
Complete Chapter 4 Hands-On Labs in Network+ Simulator Lite	156
Additional Resources	157
Review Questions	157
Chapter 5 Common Ports and Protocols	165
Foundation Topics	166
Ports and Protocols	166
DHCP (Dynamic Host Configuration Protocol)	166
DNS (Domain Name System)	166
FTP (File Transfer Protocol)	166
H.323	166
HTTP	166
HTTPS	167
IMAP	167
IMAP over SSL	167
LDAP	167
LDAPS	167
MGCP	167
MySQL	167
NTP	168
POP3	168
POP3 over SSL	168
RDP	168

	SFTP	168
	SIP	168
	SMB	168
	SMTP	169
	SMTP TLS	169
	SNMP	169
	SSH	169
	SQLnet	169
	<i>Structured Query Language (SQL) Server</i>	169
	Syslog	169
	Telnet	170
	TFTP	170
	Protocol/Port Summary	170
	IP Protocol Types	172
	Transmission Control Protocol (TCP)	172
	User Datagram Protocol (UDP)	172
	Internet Control Message Protocol (ICMP)	173
	Generic Routing Encapsulation (GRE)	173
	Internet Protocol Security (IPsec)	173
	TCP/IP Suite Protocol Summary	173
	Summary	175
	Exam Preparation Tasks	175
	Review All the Key Topics	175
	Complete Tables and Lists from Memory	176
	Define Key Terms	176
	Additional Resources	177
	Review Questions	177
Chapter 6	Network Services	181
	Foundation Topics	182
	DHCP	182
	DNS	185
	NTP	190
	Real-World Case Study	191
	Summary	191

	Exam Preparation Tasks	191
	Review All the Key Topics	191
	Complete Tables and Lists from Memory	192
	Define Key Terms	192
	Additional Resources	193
	Review Questions	193
Chapter 7	Corporate and Datacenter Architectures	197
	Foundation Topics	198
	The Three-Tiered Network Architecture	198
	The Access/Edge Layer	198
	The Distribution/Aggregation Layer	199
	The Core Layer	200
	Software-Defined Networking	200
	Spine and Leaf	202
	Storage Area Networks	204
	Deciding on an Architecture	205
	Real-World Case Study	206
	Summary	206
	Exam Preparation Tasks	206
	Review All the Key Topics	206
	Define Key Terms	207
	Additional Resources	207
	Review Questions	207
Chapter 8	Cloud Concepts	211
	Foundation Topics	212
	Deployment Models	212
	Service Models	213
	Key Cloud Concepts	214
	Infrastructure as Code (IaC)	214
	Connectivity Options	215
	Multitenancy	215
	Elasticity	215
	Scalability	216
	Cloud Security	216

Real-World Case Study	217
Summary	217
Exam Preparation Tasks	217
Review All the Key Topics	217
Define Key Terms	218
Additional Resources	218
Review Questions	218

Part II: Network Implementations

Chapter 9 Various Network Devices 221

Foundation Topics	222
Networking Devices	222
Hubs	222
Bridges	223
Layer 2 Switch	225
Layer 3 Capable Switch	231
Routers	233
Access Points	234
Wireless LAN Controller	235
Load Balancer	235
Cable Modem	235
DSL Modem	235
VPN Headend	236
Proxy Servers	237
Firewalls	238
Intrusion Detection and Prevention	239
<i>IDS Versus IPS</i>	239
<i>IDS and IPS Device Categories</i>	241
Networking Device Summary	242
Networked Devices	244
Voice over IP Protocols and Components	244
Printer	245
Physical Access Control Devices	245
Cameras	246

Heating, Ventilation, and Air Conditioning (HVAC) Sensors	246
Technologies for the Internet of Things	246
Industrial Control Systems/Supervisory Control and Data Acquisition (SCADA)	248
Real-World Case Study	248
Summary	249
Exam Preparation Tasks	249
Review All the Key Topics	249
Complete Tables and Lists from Memory	250
Define Key Terms	250
Additional Resources	251
Review Questions	251
Chapter 10 Routing Technologies and Bandwidth Management	255
Foundation Topics	256
Routing	256
Sources of Routing Information	259
Directly Connected Routes	259
Static Routes	260
Dynamic Routing Protocols	261
Routing Protocol Characteristics	263
Believability of a Route	263
Metrics	264
Interior Versus Exterior Gateway Protocols	264
Route Advertisement Method	264
Distance Vector	265
Link State	268
Routing Protocol Examples	268
Bandwidth Management	270
Introduction to QoS	271
QoS Configuration Steps	272
QoS Components	273
QoS Mechanisms	274
<i>Policing and Traffic Shaping</i>	275

Real-World Case Study	276
Summary	277
Exam Preparation Tasks	278
Review All the Key Topics	278
Complete Tables and Lists from Memory	278
Define Key Terms	278
Additional Resources	279
Review Questions	279
Chapter 11 Ethernet Switching	283
Foundation Topics	284
Principles of Ethernet	284
Ethernet Origins	284
Carrier-Sense Multiple Access with Collision Detection	286
Distance and Speed Limitations	290
Ethernet Switch Features	292
Virtual LANs	293
Switch Configuration for an Access Port	295
Trunks	296
Switch Configuration for a Trunk Port	297
Spanning Tree Protocol	298
Corruption of a Switch's MAC Address Table	299
Broadcast Storms	300
STP Operation	301
Link Aggregation	304
LACP Configuration	305
Power over Ethernet	306
Port Monitoring	307
Port Mirroring Configuration	309
User Authentication	309
Management Access and Authentication	311
First-Hop Redundancy	312
Other Switch Features	313
Real-World Case Study	314

Summary	315
Exam Preparation Tasks	315
Review All the Key Topics	315
Complete Tables and Lists from Memory	316
Define Key Terms	316
Additional Resources	317
Review Questions	317
Chapter 12 Wireless Standards	321
Foundation Topics	322
Introducing Wireless LANs	322
WLAN Concepts and Components	322
Wireless Routers	322
Wireless Access Point	323
Antennas	324
Frequencies and Channels	327
CSMA/CA	329
Transmission Methods	330
WLAN Standards	331
802.11a	331
802.11b	331
802.11g	331
802.11n (Wi-Fi 4)	332
802.11ac (Wi-Fi 5)	332
802.11ax (Wi-Fi 6)	332
802.11x Standard Summary	333
Deploying Wireless LANs	334
Types of WLANs	334
IBSS	334
BSS	335
ESS	335
Mesh Topology	336
Sources of Interference	336
Wireless AP Placement	338

Securing Wireless LANs	339
Security Issues	339
Approaches to WLAN Security	341
Security Standards	343
WEP	343
WPA	344
WPA2	345
Additional Wireless Options	345
Real-World Case Study	345
Summary	346
Exam Preparation Tasks	346
Review All the Key Topics	346
Complete Tables and Lists from Memory	347
Define Key Terms	347
Additional Resources	348
Review Questions	348

Part III: Network Operations

Chapter 13 Ensure Network Availability 353

Foundation Topics	354
Monitoring Tools	354
Performance Metrics/Sensors	354
SNMP	356
Additional Monitoring Topics	360
Syslog	361
Logs	363
Application Logs	363
Security Logs	364
System Logs	364
Environmental Monitor	365
Interface Statistics/Status	365
NetFlow	368
Real-World Case Study	368
Summary	368
Exam Preparation Tasks	369

Review All the Key Topics	369
Complete Tables and Lists from Memory	369
Define Key Terms	370
Additional Resources	370
Review Questions	370
Chapter 14 Organizational Documents and Policies	375
Foundation Topics	376
Plans and Policies	376
Change Management	376
Incident Response Plan	376
Disaster Recovery and Business Continuity Policies	377
System Life Cycle	377
Hardening and Security Policies	378
Password Policy	378
Security Policies	379
Data Loss Prevention	380
Remote Access Policies	381
Bring-Your-Own-Device (BYOD) Policy	382
Acceptable Use Policy (AUP)	382
Safety Procedures	383
Privileged User Agreement (PUA)	383
Onboarding/Offboarding Procedures	384
Licensing Restrictions	384
International Export Controls	385
Non-Disclosure Agreement (NDA)	385
Common Documentation	385
Real-World Case Study	387
Summary	388
Exam Preparation Tasks	388
Review All the Key Topics	388
Define Key Terms	389
Additional Resources	389
Review Questions	390

Chapter 15 High Availability and Disaster Recovery 393

- Foundation Topics 394
- High Availability 394
 - High Availability (HA) Measurement 394
 - MTTR, MTBF, RTO, and RPO 394
 - Fault-Tolerant Network Design 395
 - Hardware Redundancy 397
 - Layer 3 Redundancy 398
 - Design Considerations for High-Availability Networks 399
 - High-Availability Best Practices 400
 - Content Caching 401
 - Load Balancing 401
 - Hardware Redundancy 402
- Real-World Case Study: SOHO Network Design 403
 - Case Study Scenario 403
 - Suggested Solution 405
 - IP Addressing 405
 - Layer 1 Media 406
 - Layer 2 Devices 407
 - Layer 3 Devices 408
 - Wireless Design 408
 - Environmental Factors 409
 - Cost Savings Versus Performance 409
 - Topology 410
- Real-World Case Study 410
- Summary 411
- Exam Preparation Tasks 411
- Review All the Key Topics 411
- Define Key Terms 412
- Additional Resources 412
- Review Questions 413

Part IV: Network Security**Chapter 16 Common Security Concepts 417**

Foundation Topics 418

Core Security Concepts 418

Confidentiality, Integrity, and Availability (CIA) 418

Confidentiality 418

Symmetric Encryption 419*Asymmetric Encryption* 420

Integrity 422

Availability 423

Threats, Vulnerabilities, and Exploits 423

Threats 423*Vulnerabilities* 423*Exploits* 424

Least Privilege 425

Role-Based Access 425

Zero Trust 426

Defense in Depth 426

Network Segmentation Enforcement 427*Screened Subnet* 427*Separation of Duties* 427*Network Access Control* 427*Honeypot* 428

Authentication Methods 428

Multifactor 428

TACACS+ 429

Single Sign-On 429

RADIUS 429

LDAP 429

Kerberos 429

Local Authentication 430

802.1X 430

EAP 431

Risk Management and SIEM	431
Risk Management	431
Security Risk Assessments	431
<i>Threat Assessment</i>	431
<i>Vulnerability Assessment</i>	432
<i>Penetration Testing</i>	432
<i>Posture Assessment</i>	432
Business Risk Assessment	432
<i>Process Assessment</i>	432
<i>Vendor Assessment</i>	433
Security Information and Event Management (SIEM)	433
Real-World Case Study	434
Summary	434
Exam Preparation Tasks	434
Review All the Key Topics	434
Define Key Terms	435
Additional Resources	435
Review Questions	436
Chapter 17 Common Types of Attacks	439
Foundation Topics	440
Technology-Based Attacks	440
Denial of Service	440
Distributed Denial of Service	441
On-Path Attack (Formerly Known as Man-in-the-Middle Attack)	441
DNS Poisoning	442
VLAN Hopping	442
ARP Spoofing	442
Rogue DHCP	442
Rogue Access Point	443
Evil Twin	443
Ransomware	443
Password Attacks	443
MAC Spoofing	444

IP Spoofing	444
Deauthentication	444
Malware	444
Human and Environmental Attacks	445
Other Miscellaneous Attacks	445
Real-World Case Study	449
Summary	449
Exam Preparation Tasks	449
Review All the Key Topics	449
Define Key Terms	450
Complete Chapter 17 Hands-On Lab in Network+ Simulator Lite	450
Additional Resources	450
Review Questions	450
Chapter 18 Network Hardening Techniques	453
Foundation Topics	454
Best Practices	454
Wireless Security and IoT Considerations	458
Real-World Case Study	459
Summary	460
Exam Preparation Tasks	460
Review All the Key Topics	460
Define Key Terms	460
Additional Resources	461
Review Questions	461
Chapter 19 Remote Access Methods	465
Foundation Topics	466
Virtual Private Networks (VPNs)	466
Overview of IPsec with IKEv1	468
IKE Modes and Phases	469
Authentication Header and Encapsulating Security Payload	470
The Five Steps in Setting Up and Tearing Down an IPsec Site-to-Site VPN Using IKEv1	472
IKEv2	473
Other VPN Technologies	473

- Other Remote Access Technologies 474
- Authentication and Authorization Considerations 478
- In-Band vs. Out-of-Band Management 479
- Real-World Case Study 480
- Summary 480
- Exam Preparation Tasks 480
- Review All the Key Topics 480
- Complete Tables and Lists from Memory 481
- Define Key Terms 481
- Complete Chapter 19 Hands-On Lab in Network+ Simulator Lite 481
- Additional Resources 481
- Review Questions 482

Chapter 20 Physical Security 485

- Foundation Topics 486
- Detection Methods 486
- Prevention Methods 486
- Asset Disposal 489
- Real-World Case Study 490
- Summary 490
- Exam Preparation Tasks 490
- Review All the Key Topics 490
- Define Key Terms 491
- Additional Resources 491
- Review Questions 491

Part V: Network Troubleshooting

Chapter 21 A Network Troubleshooting Methodology 495

- Foundation Topics 496
- Troubleshooting Basics 496
 - Troubleshooting Fundamentals 496
 - Structured Troubleshooting Methodology 498
- Real-World Case Study 501
- Summary 501
- Exam Preparation Tasks 501
- Review All the Key Topics 501

Complete Tables and Lists from Memory	502
Define Key Terms	502
Additional Resource	502
Review Questions	502
Chapter 22 Troubleshoot Common Cabling Problems	505
Foundation Topics	506
Specifications and Limitations	506
Cable Considerations and Applications	506
Common Issues	507
Common Tools	509
Real-World Case Study	514
Summary	514
Exam Preparation Tasks	514
Review All the Key Topics	514
Define Key Terms	515
Additional Resources	515
Review Questions	515
Chapter 23 Network Software Tools and Commands	519
Foundation Topics	520
Software Tools	520
WiFi Analyzer	520
Protocol Analyzer/Packet Capture	520
Bandwidth Speed Tester	520
Port Scanner	521
iperf	521
NetFlow Analyzers	522
TFTP Server	522
Terminal Emulator	522
IP Scanner	522
Command Line Tools	522
ping	523
ping with IPv6	524
ipconfig	524
ifconfig	528

ip	529
nslookup	529
dig	531
tracert	532
tracert for IPv6	533
arp	533
netstat	535
hostname	537
route	538
telnet	542
tcpdump	542
nmap	542
Basic Network Platform Commands	543
Real-World Case Study	543
Summary	543
Exam Preparation Tasks	544
Review All the Key Topics	544
Complete Tables and Lists from Memory	544
Define Key Terms	545
Additional Resource	545
Review Questions	545
Chapter 24 Troubleshoot Common Wireless Issues	549
Foundation Topics	550
Specifications and Limitations	550
Considerations	551
Antennas	551
Frequencies and Channels	552
Other Considerations	552
Common Issues	553
Wireless Network Troubleshooting	554
Wireless Network Troubleshooting Solution	555
Real-World Case Study	556

	Summary	556
	Exam Preparation Tasks	556
	Review All the Key Topics	556
	Define Key Terms	557
	Review Questions	557
Chapter 25	Troubleshoot General Network Issues	561
	Foundation Topics	562
	Considerations for General Network Troubleshooting	562
	Common Issues	563
	Real-World Case Study	566
	Summary	567
	Exam Preparation Tasks	567
	Review All the Key Topics	567
	Define Key Terms	567
	Additional Resources	568
	Review Questions	568
Part VI: Final Preparation		
Chapter 26	Final Preparation	571
	Tools for Final Preparation	571
	Video Training	572
	Memory Tables	572
	Simulations and Performance-Based Exercises	573
	End-of-Chapter Review Tools	573
	Suggested Plan for Final Review and Study	574
	Strategies for Taking the Exam	576
	Summary	577
	Glossary of Key Terms	579
APPENDIX A	Answers to Review Questions	623
APPENDIX B	CompTIA Network+ (N10-008) Cert Guide Exam Updates	639
	Index	641

ONLINE ELEMENTS:

APPENDIX C Memory Tables

APPENDIX D Memory Tables Answer Key

APPENDIX E Study Planner

Exam Essentials Interactive Study Guide

Key Terms Flash Cards Application

Instructional Videos

Performance-Based Exercises

CompTIA Network+ N10-008 Hands-On Lab Simulator Lite Software

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 Splunk. He is an avid tennis player, a private pilot, and a semi-professional poker player, and he loves anything at all to do with technology.

Dedication

This book is dedicated to my wife, Joette Sequeira, who made this book, and all the rest of them, possible.

Acknowledgments

I cannot thank Brett Bartow and Chris Cleveland enough for their patience as I created this latest edition of the text.

About the Technical Reviewer

Chris Crayton (MCSE) is an author, technical consultant, and trainer. In the past, 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 leading publishing companies. Chris holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

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

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. 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
- Performance-based exercises
- CompTIA Network+ Hands-on Lab Simulator Lite Software for exam N10-008
- The Pearson Test Prep practice test software
- 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 <http://www.pearsonitcertification.com/register>.
- 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 your book 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.

Pearson Test Prep Practice Test Software

The companion website that accompanies this book includes the Pearson Test Prep practice test engine, which is software that displays and grades a set of exam-realistic practice test questions. Using the Pearson Test Prep practice test engine, you can either study by going through the questions in study mode or take a simulated CompTIA Network+ exam that mimics real exam conditions. The software also has a flash card mode that allows you to challenge yourself to answer the questions without seeing the multiple-choice answers.

The Pearson Test Prep software is available both online and as a Windows desktop application that you can run offline. The online version can be accessed at www.pearsonestprep.com. This version can be used on any device that has an Internet

connection, including desktop computers, laptop computers, tablets, and smartphones. It is optimized for viewing on screens as small as a standard iPhone screen. The desktop application can be downloaded and installed from the companion website.

NOTE The desktop Pearson Test Prep application is a Windows-based application, so it is only designed to run on Windows. Although it can be run on other operating systems using a Windows emulator, other operating systems are not officially supported for the desktop version. If you are using an OS other than Windows, you might want to consider using the online version of Pearson Test Prep instead.

Accessing the test engine is a two-step process. The first step is to either install the software on your desktop or access the online version website. However, the practice exam (that is, the database of CompTIA Network+ exam questions) is not available to you until you take the second step: Register the unique access code that accompanies your book.

NOTE The cardboard sleeve in the back of the physical book includes a piece of paper. The paper lists the *access code* for the practice exam associated with this book. Make sure you keep the access code even after you have registered your practice exam because you may need to refer to it later. Also, on the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the *CompTIA Network+ Cert Guide, Premium Edition eBook and Practice Test* product—a \$40 value!

Installing the Pearson Test Prep Software

If you choose to use the Windows desktop version of the practice test software, you will need to download the installers from the companion website.

The software installation process is similar to other wizard-based installation processes. If you have already installed the Pearson Test Prep practice test software from another Pearson product, you do not need to reinstall the software. Just launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in sleeve in the back of the book. The following steps outline the installation process:

- Step 1.** Download the software to your computer from the companion website.
- Step 2.** Extract all files from the .zip file you downloaded.
- Step 3.** Launch the installer from the extracted files folder.
- Step 4.** Respond to the wizard-based prompts.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the back of book sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please register when prompted. If you already have a Pearson website login, you do not need to register again; just use your existing login.

Activating and Downloading the Practice Exam

The second step to accessing your practice exam product is to activate the product using the unique access code found in the back of book sleeve. You must follow this step regardless of which version of the product you are using—the online version or the Windows desktop version. The following steps walk you through how to activate your exam on each platform.

Windows Desktop Version:

1. Start the Pearson Test Prep Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, on the My Products or Tools tab, click the **Activate** button.
3. At the next screen, enter the *access code* from the paper inside the cardboard sleeve in the back of the book and then click the **Activate** button. The activation process downloads the practice exam to your machine.
4. Click **Next** and then click **Finish**.

Online Version:

1. On a device with an active Internet connection, open your browser of choice and go to the website **www.pearsonestprep.com**.
2. Select **Pearson IT Certification** as the product group.
3. Enter the email address and password associated with your account and click **Login**.
4. In the middle of the screen, click the **Activate New Product** button.
5. Enter the access code from the paper inside the cardboard sleeve in the back of the book and click the **Activate** button.

After the activation process is complete, the My Products tab should list your new exam. If you do not see the exam, make sure that you selected the **My Products** tab

on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Exams** button.

To update an exam that you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Updating your exams ensures that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the **Tools** tab and click the **Update Application** button to ensure that you are running the latest version of the exam engine.

NOTE The online version always contains the latest updates to the exam questions, so there is never a need to update when you're using that version.

Activating Other Exams

The exam software installation process and the registration process both occur only once. Then, for each new exam, only a few steps are required. For example, if you buy another new Pearson IT Certification Cert Guide, you can extract the activation code from the sleeve in the back of that book, start the exam engine (if it's not still up and running), and perform the activation steps from the previous list.

Premium Edition

In addition to the free practice exam provided with the book, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional two full practice exams and an eBook (in PDF, EPUB, and Kindle formats). Also, the Premium Edition title provides remediation for each question that links to the specific part of the eBook that relates to that question.

If you purchased the print version of this title, you can purchase the Premium Edition at a deep discount. You'll find a coupon code in the back of book sleeve that contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the Premium Edition product page, go to <http://www.pearsonitcertification.com>.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the Network+ N10-008 blueprint from CompTIA. This book also helps you prepare for the N10-008 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 N10-008 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 on the book’s companion website in Appendixes C and D. 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.
- **Exercises:** This book comes with 40 performance-based practice exercises that are designed to help you prepare for the hands-on portion of the Network+ exam. These exercises are available on the companion website. Make sure you do the exercises as you complete each chapter and again when you have completed the book and are doing your final preparation.
- **Hands-on labs:** These hands-on exercises, which are an important part of this book, include matching, drag and drop, and simulations. In addition to reading this book, you should go through all the exercises included with the book. These interactive hands-on exercises provide examples, additional information, and insight about a vendor’s implementation of the technologies. To perform the labs, simply install the CompTIA Network+ N10-008 Hands-on Lab Simulator Lite software. This software is a Windows and Mac desktop application. You should be sure to install the software prior to reading the book because each chapter will indicate what labs you should perform. To install the software, follow these steps:
 - Step 1.** Go to the companion website for the book. (Refer to the “Resources” section for how to access the companion website.)

- Step 2.** Click the link to download the CompTIA Network+ N10-008 Hands-on Lab Simulator Lite software.
 - Step 3.** Once you have downloaded the software to your computer, extract all the files from the .zip file.
 - Step 4.** Launch the installer from the extracted files.
 - Step 5.** Respond to the wizard-based prompts.
- **Practice exams:** 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. You can access both the online and desktop versions using the access code printed on the card in the sleeve in the back of this book. 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.
 - **Exam essentials:** This book includes an exam essentials appendix that summarizes the key points from every chapter. This review tool is available in print and as an interactive PDF on the companion website. Review these essential exam facts after each chapter and again when you have completed the book. This makes a great review summary that you can mark up as you review and master each concept.

For current information about the CompTIA Network+ certification exam, visit <https://certification.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 hands-on labs and 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.

Make sure you complete all the performance-based question exercises and hands-on labs associated with this book. The exercises and labs are organized by chapter, making it easy to perform them after you complete each section. These exercises help you reinforce what you have learned, offer examples of some popular vendors' methods for implementing networking technologies, and provide additional information to assist you in building real-world skills and preparing you for the certification exam.

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

Use the practice exam, which is included on this book's companion website. As you work through the practice exam, 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 exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions become, and the less accurately the practice exam judges your skills.

After you work through the practice exam a second time and feel confident with your skills, schedule the real CompTIA Network+ exam (N10-008).

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (*objectives*) and specific topics under each general topic (*subobjectives*) for the CompTIA Network+ N10-008 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	N10-008 Exam Objective	N10-008 Exam Subobjective
1 The OSI Model and Encapsulation	1.0 Networking Fundamentals	1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
2 Network Topologies and Types	1.0 Networking Fundamentals	1.2 Explain the characteristics of network topologies and network types.

Chapter	N10-008 Exam Objective	N10-008 Exam Subobjective
3 Network Media Types	1.0 Networking Fundamentals	1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
4 IP Addressing	1.0 Networking Fundamentals	1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.
5 Common Ports and Protocols	1.0 Networking Fundamentals	1.5 Explain common ports and protocols, their application, and encrypted alternatives.
6 Network Services	1.0 Networking Fundamentals	1.6 Explain the use and purpose of network services.
7 Corporate and Datacenter Architectures	1.0 Networking Fundamentals	1.7 Explain basic corporate and datacenter network architecture.
8 Cloud Concepts	1.0 Networking Fundamentals	1.8 Summarize cloud concepts and connectivity options.
9 Various Network Devices	2.0 Network Implementations	2.1 Compare and contrast various devices, their features and their appropriate placement on the network.
10 Routing Technologies and Bandwidth Management	2.0 Network Implementations	2.2 Compare and contrast routing technologies and bandwidth management concepts.
11 Ethernet Switching	2.0 Network Implementations	2.3 Given a scenario, configure and deploy common Ethernet switching features.
12 Wireless Standards	2.0 Network Implementations	2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.
13 Ensure Network Availability	3.0 Network Operations	3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
14 Organizational Documents and Policies	3.0 Network Operations	3.2 Explain the purpose of organizational documents and policies.
15 High Availability and Disaster Recovery	3.0 Network Operations	3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

Chapter	N10-008 Exam Objective	N10-008 Exam Subobjective
16 Common Security Concepts	4.0 Network Security	4.1 Explain common security topics.
17 Common Types of Attacks	4.0 Network Security	4.2 Compare and contrast common types of attacks.
18 Network Hardening Techniques	4.0 Network Security	4.3 Given a scenario, apply network hardening techniques.
19 Remote Access Methods	4.0 Network Security	4.4 Compare and contrast remote access methods and security implications.
20 Physical Security	4.0 Network Security	4.5 Explain the importance of physical security.
21 A Network Troubleshooting Methodology	5.0 Network Troubleshooting	5.1 Explain the network troubleshooting methodology.
22 Troubleshoot Common Cabling Problems	5.0 Network Troubleshooting	5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.
23 Network Software Tools and Commands	5.0 Network Troubleshooting	5.3 Given a scenario, use the appropriate network software tools and commands.
24 Troubleshoot Common Wireless Issues	5.0 Network Troubleshooting	5.4 Given a scenario, troubleshoot common wireless connectivity issues.
25 Troubleshoot General Network Issues	5.0 Network Troubleshooting	5.5 Given a scenario, troubleshoot general 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**—The OSI model is an extremely powerful guide you can use as you design, implement, and troubleshoot networks.
- **Chapter 2: Network Topologies and Types**—This chapter explores the many types of networks and topologies used in enterprises today.
- **Chapter 3: Network Media Types**—This chapter drills deep into the media that connects networks today.
- **Chapter 4: IP Addressing**—Addressing of systems is critical in networks, and this chapter covers the addressing used with IPv4 and IPv6.
- **Chapter 5: Common Ports and Protocols**—This chapter introduces many of the common ports and protocols in use today.
- **Chapter 6: Network Services**—The network is the plumbing that carries the data and services you require. This chapter examines some of the many services that you will encounter in networks today.
- **Chapter 7: Corporate and Datacenter Architectures**—Today's corporate enterprise networks and the datacenters that are common in networks today are the subject of this chapter.
- **Chapter 8: Cloud Concepts**—This chapter explores key principles of the cloud, which has become common in networks today.
- **Chapter 9: Various Network Devices**—This chapter explores some of the various devices found in networks today.
- **Chapter 10: Routing Technologies and Bandwidth Management**—Moving packets from one network to another is the job of a router. This chapter ensures that you are well versed in the many technologies that operate in this category.
- **Chapter 11: Ethernet Switching**—Wireless is great, but Ethernet still rules the access layer. This chapter explores Ethernet in depth.
- **Chapter 12: Wireless Standards**—Wireless networking is here to stay. This chapter provides you with details on important topics such as security and emerging technologies.

- **Chapter 13: Ensure Network Availability**—There are many tools available today to help you ensure that a network is running smoothly. This chapter details many of them.
- **Chapter 14: Organizational Documents and Policies**—This chapter discusses many of the documents and policies that are found in enterprises today. Those that could impact the IT department are the focus of this chapter.
- **Chapter 15: High Availability and Disaster Recovery**—Making sure the network is always available is the subject of this chapter.
- **Chapter 16: Common Security Concepts**—This chapter explores the fundamentals of network security.
- **Chapter 17: Common Types of Attacks**—This chapter covers the most common types of attacks in the cybersecurity landscape today.
- **Chapter 18: Network Hardening Techniques**—This chapter explores the methods of hardening the network and its devices against the most common attacks.
- **Chapter 19: Remote Access Methods**—This chapter explores the many types of remote access that are possible today.
- **Chapter 20: Physical Security**—This chapter explores the important topic of physical security for a network.
- **Chapter 21: A Network Troubleshooting Methodology**—Whereas other chapters just touch on network troubleshooting, this chapter makes it the focus.
- **Chapter 22: Troubleshoot Common Cabling Problems**—This chapter examines the most common issues with network media and what you can do to detect and resolve these issues.
- **Chapter 23: Network Software Tools and Commands**—This chapter explores many of the common tools and commands you can use to troubleshoot a network.
- **Chapter 24: Troubleshoot Common Wireless Issues**—This chapter explores the most common issues with wireless networks.
- **Chapter 25: Troubleshoot General Network Issues**—This chapter explores common general network issues and how you can quickly detect and resolve them.

Routing Technologies and Bandwidth Management

In Chapter 4, “IP Addressing,” you learned how Internet Protocol (IP) networks can be divided into subnets. Each subnet is its own broadcast domain, and the device that separates broadcast domains is a router (which this text considers synonymous with a multilayer switch). A multilayer switch is a network device that can perform the Layer 2 switching of frames as well as the Layer 3 routing of IP packets. Multilayer switches generally use dedicated chips to perform these functions and, as a result, may be faster than traditional routers in forwarding packets.

For traffic to flow between subnets, the traffic has to be routed; this routing is a router’s primary job. This chapter discusses how routing occurs and introduces a variety of approaches for performing routing, including dynamic routing, static routing, and default routing. The chapter also breaks down the various categories of routing protocols and provides specific examples of each.

The chapter concludes with a discussion of various bandwidth management topics, including a discussion of QoS concepts, such as traffic shaping.

Foundation Topics

Routing

To understand basic routing processes, consider Figure 10-1. In this topology, PC1 needs to send traffic to Server1. Notice that these devices are on different networks. In this topology, how does a packet from the source IP address 192.168.1.2 get routed to the destination IP address 192.168.3.2?

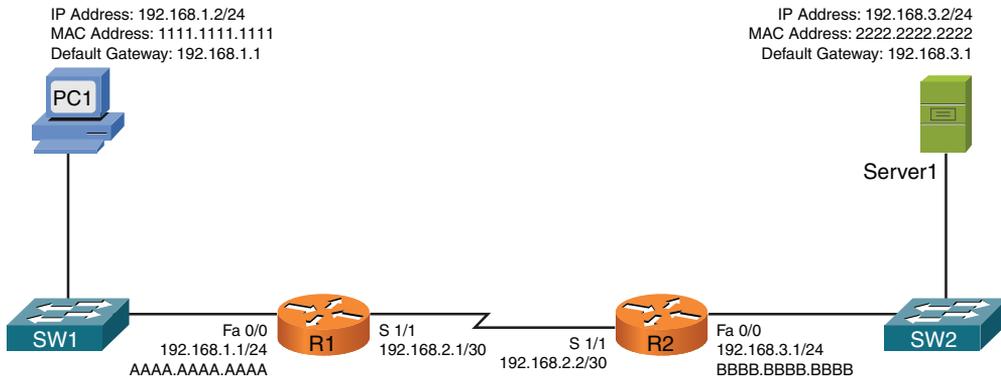


FIGURE 10-1 Basic Routing Topology

It might help to walk through this process systematically:

Key Topic

- Step 1.** PC1 compares its IP address and subnet mask 192.168.1.2/24 with the destination IP address and subnet mask 192.168.3.2/24. PC1 concludes that the destination IP address resides on a remote subnet. Therefore, PC1 needs to send the packet to its default gateway, which could have been manually configured on PC1 or dynamically learned via Dynamic Host Configuration Protocol (DHCP). In this example, PC1 has the default gateway 192.168.1.1 (router R1). However, to construct a Layer 2 frame, PC1 also needs the MAC address of its default gateway. PC1 sends an *Address Resolution Protocol (ARP)* request for router R1's MAC address. After PC1 receives an ARP reply from router R1, PC1 adds router R1's MAC address to its ARP cache. PC1 now sends its data in a frame destined for Server1, as shown in Figure 10-2.

NOTE ARP is a broadcast-based protocol and, therefore, does not travel beyond the local subnet of the sender.

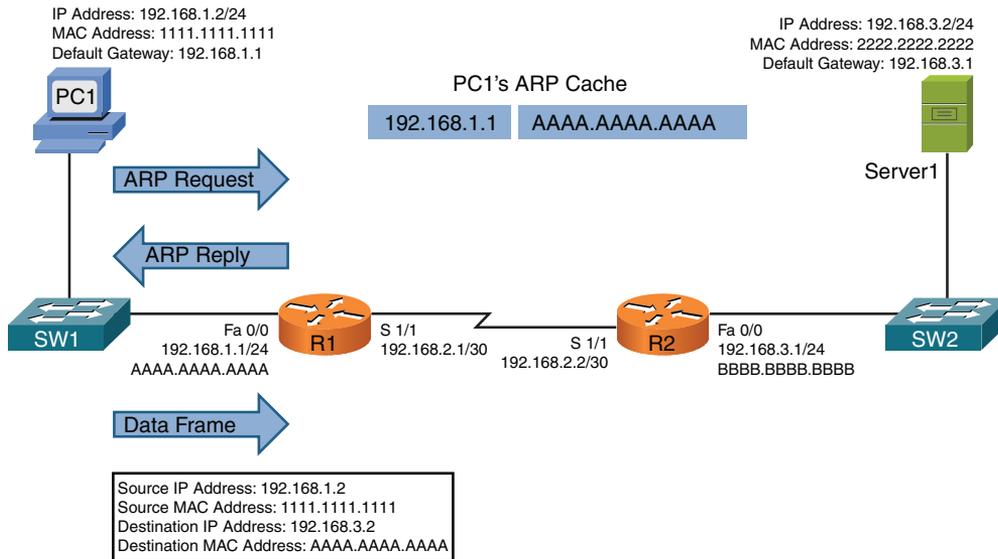


FIGURE 10-2 Basic Routing: Step 1

- Step 2.** Router R1 receives the frame sent from PC1 and interrogates the IP header. An IP header contains a *Time-to-Live (TTL)* field, which is decremented once for each router hop. Therefore, router R1 decrements the packet's TTL field. If the value in the TTL field is reduced to 0, the router discards the frame and sends a "time exceeded" Internet Control Message Protocol (ICMP) message back to the source. As long as the TTL has not been decremented to 0, router R1 checks its routing table to determine the best path to reach network 192.168.3.0/24. In this example, router R1's routing table has an entry stating that network 192.168.3.0/24 is accessible via interface Serial 1/1. Note that ARP is not required for serial interfaces because these interface types do not have MAC addresses. Router R1, therefore, forwards the frame out its Serial 1/1 interface, as shown in Figure 10-3.

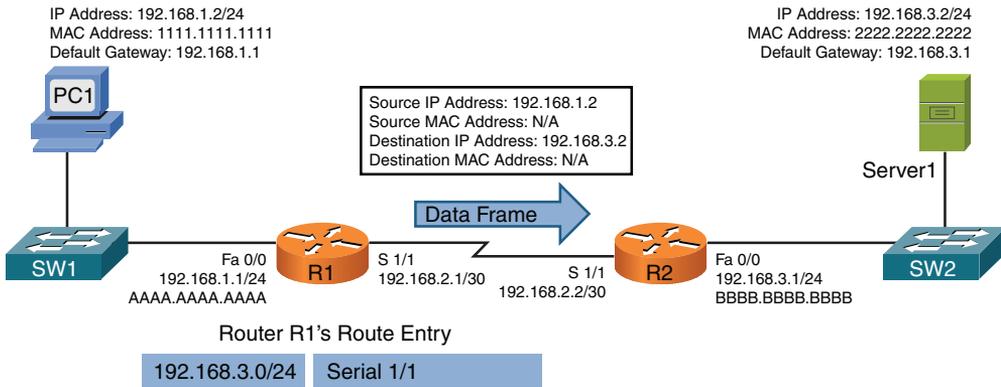


FIGURE 10-3 Basic Routing: Step 2

Step 3. When router R2 receives the frame, it decrements the TTL in the IP header, just as router R1 did. Again, as long as the TTL has not been decremented to 0, router R2 interrogates the IP header to determine the destination network. In this case, the destination network 192.168.3.0/24 is directly attached to router R2's Fast Ethernet 0/0 interface. Similar to the way PC1 sent out an ARP request to determine the MAC address of its default gateway, router R2 sends an ARP request to determine the MAC address of Server1. After an ARP reply is received from Server1, router R2 forwards the frame out its Fast Ethernet 0/0 interface to Server1, as illustrated in Figure 10-4.

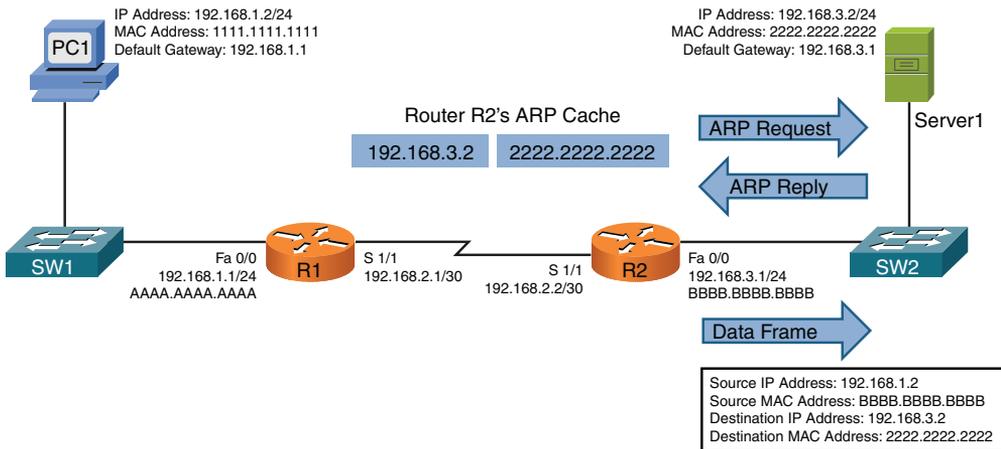


FIGURE 10-4 Basic Routing: Step 3

The previous steps identified two router data structures:

- **IP routing table:** When a router needed to route an IP packet, it consulted its IP routing table to find the best match. The best match is the route that has the longest prefix. Specifically, a route entry with the longest prefix is the most specific network. For example, imagine that a router has an entry for network 10.0.0.0/8 and for network 10.1.1.0/24. Also, imagine that the router is seeking the best match for destination address 10.1.1.1/24. The router would select the 10.1.1.0/24 route entry as the best entry because that route entry has the longest prefix (/24 is longer than /8, which is a more specific entry).
- **Layer 3 to Layer 2 mapping:** In the previous example, router R2's ARP cache contained Layer 3 to Layer 2 mapping information. Specifically, the ARP cache had a mapping that said MAC address 2222.2222.2222 corresponded to IP address 192.168.3.2.

As shown in the preceding example, routers rely on their internal routing table to make packet-forwarding decisions. So how does a router's routing table become populated with entries? That is the focus of the next section.

Sources of Routing Information

A router's routing table can be populated from various sources. As an administrator, you could statically configure a route entry. A route could be learned via a *dynamic routing* protocol (for example, OSPF or EIGRP), or a router could know how to get to a specific network because the router is physically attached to that network.

Directly Connected Routes

A router that has an interface directly participating in a network knows how to reach that specific destination network. For example, consider Figure 10-5.

In Figure 10-5, router R1's routing table knows how to reach the 192.168.1.0/24 and 192.168.2.0/30 networks because router R1 has an interface physically attached to each network. Similarly, router R2 has interfaces participating in the 10.1.1.0/30 and 192.168.2.0/30 networks and therefore knows how to reach those networks. The entries currently shown to be in the routing tables of routers R1 and R2 are called *directly connected routes*.

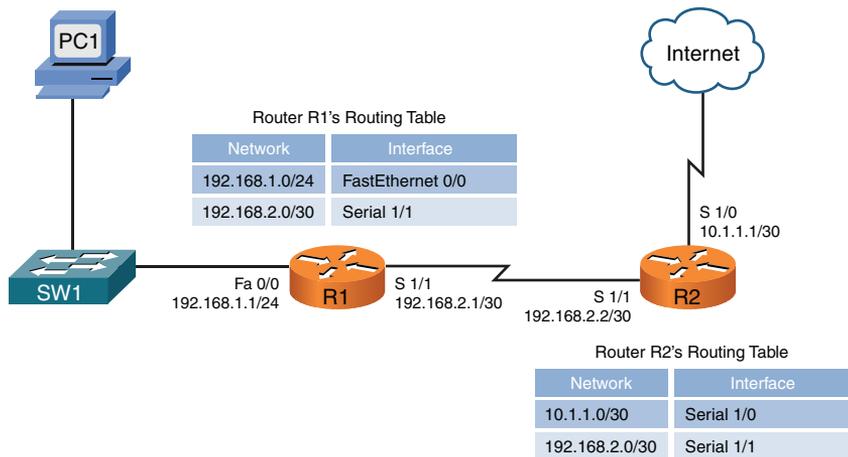


FIGURE 10-5 Directly Connected Routes

Static Routes

It is also possible to statically configure routes in a router's routing table. Continuing to expand on the previous example, consider router R1. As shown in Figure 10-6, router R1 does not need knowledge of each route on the Internet. Specifically, router R1 already knows how to reach devices on its locally attached networks. All router R1 really needs to know at this point is how to get out to the rest of the world. As you can see from Figure 10-6, any traffic destined for a nonlocal network (for example, any of the networks available on the public Internet) can simply be sent to router R2. Because R2 is the next router hop along the path to reach all those other networks, router R1 could be configured with a **default static route**, which says, "If traffic is destined for a network not currently in the routing table, send that traffic out interface Serial 1/1."

NOTE A static route does not always reference a local interface. Instead, a static route might point to a **next-hop IP address** (that is, an interface's IP address on the next router to which traffic should be forwarded). The network address of a default route is 0.0.0.0/0.

Similarly, router R2 can reach the Internet by sending traffic out its Serial 1/0 interface. However, router R2 does need information about how to reach the 192.168.1.0/24 network available off router R1. To educate router R2 about how this network can be reached, a network administrator can add a static route pointing to 192.168.1.0/24 to router R2's routing table.

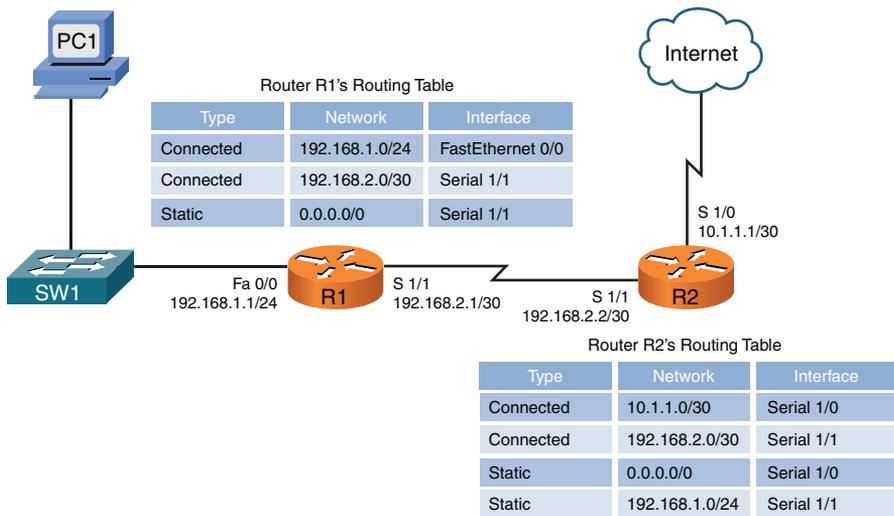


FIGURE 10-6 Static Routes

Dynamic Routing Protocols

In complex networks, such as the topology shown in Figure 10-7, static routing does not scale well. Fortunately, a variety of dynamic routing protocols are available that allow a router's routing table to be updated as network conditions change.

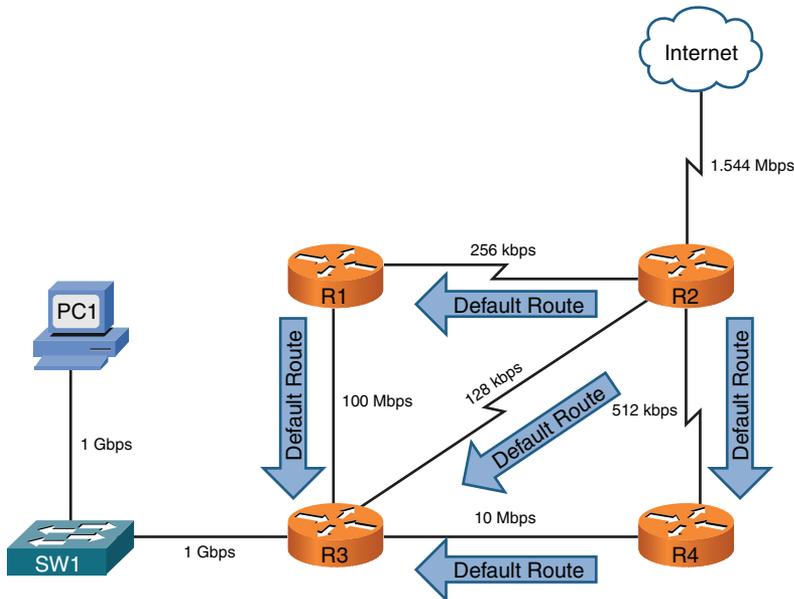


FIGURE 10-7 Dynamic Routes

In Figure 10-7, router R2 is advertising a default route to its neighbors (routers R1, R3, and R4). What happens if PC1 wants to send traffic to the Internet? PC1's default gateway is router R3, and router R3 has received three default routes. Which one does it use?

Router R3's path selection depends on the dynamic routing protocol being used. As you will see later in this chapter, a routing protocol such as Routing Information Protocol (RIP) would make the path selection based on the number of routers that must be used to reach the Internet (that is, *hop count*). Based on the topology presented, router R3 would select the 128Kbps link (where Kbps stands for kilobits per second, meaning thousands of bits per second) connecting to router R2 because the Internet would be only one hop away. If router R3 instead selected a path pointing to either router R1 or R4, the Internet would be two hops away.

However, based on the link bandwidths, you can see that the path from router R3 to router R2 is suboptimal. Unfortunately, RIP does not consider available bandwidth when making its route selection. Some other protocols, such as Open Shortest Path First (OSPF), can consider available bandwidth when making their routing decisions.

Dynamic routes also allow a router to reroute around a failed link. For example, in Figure 10-8, router R3 prefers to reach the Internet via router R4. However, the link between routers R3 and R4 goes down. Thanks to a dynamic routing protocol, router R3 knows of two other paths to reach the Internet, and it selects the next-best path, which is via router R1 in this example. This process of failing over from one route to a backup route is called *convergence*.

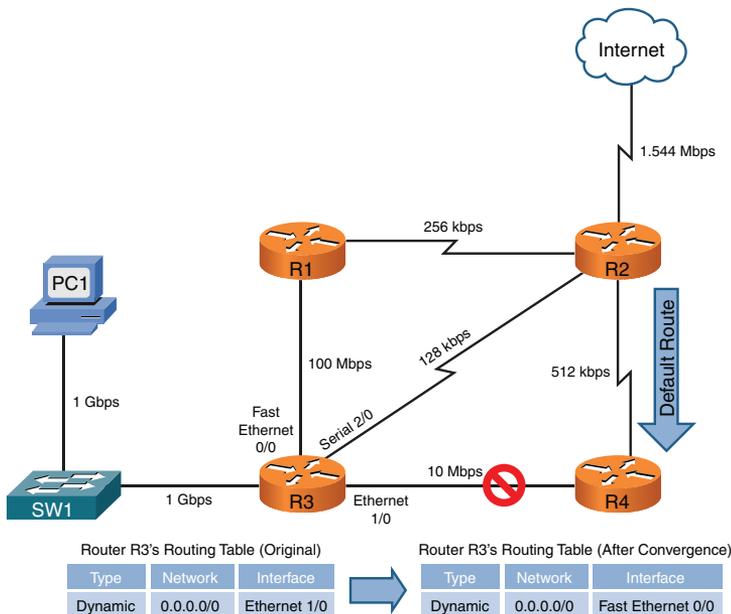


FIGURE 10-8 Route Redundancy

Routing Protocol Characteristics

Before examining the characteristics of routing protocols, we need to look at the important distinction between a *routing protocol* and a *routed protocol*:

- A ***routing protocol*** (for example, RIP, OSPF, or EIGRP) is a protocol that advertises route information between routers.
- A ***routed protocol*** is a protocol with an addressing scheme (for example, IP) that defines different network addresses. Traffic can then be routed between defined networks, perhaps with the assistance of a routing protocol.

This section looks at routing protocol characteristics, such as how believable a routing protocol is compared to other routing protocols. In addition, in the presence of multiple routes, different routing protocols use different *metrics* to determine the best path. A distinction is made between *interior gateway protocols (IGPs)* and *exterior gateway protocols (EGPs)*. Finally, this section discusses different approaches to making route advertisements.

Believability of a Route

If a network is running more than one routing protocol (maybe as a result of a corporate merger), and a router receives two route advertisements from different routing protocols for the same network, which route advertisement does the router believe? Interestingly, some routing protocols are considered to be more believable than others. For example, a Cisco router would consider EIGRP to be more believable than RIP.

The index of believability is called ***administrative distance (AD)***. Table 10-1 shows the AD values for various sources of routing information. Note that lower AD values are more believable than higher AD values.



Table 10-1 Administrative Distance

Routing Information Source	AD Value
Directly connected network	0
Statically configured network	1
EIGRP	90
OSPF	110
RIP	120
External EIGRP	170
Unknown or unbelievable	255 (considered to be unreachable)

Metrics

Some networks might be reachable via more than one path. If a routing protocol knows of multiple paths to reach such a network, which route (or routes) does the routing protocol select? Actually, it varies depending on the routing protocol and what that routing protocol uses as a *metric* (that is, a value assigned to a route). Lower metrics are preferred over higher metrics.

Some routing protocols support load balancing across equal-cost paths; this is useful when a routing protocol knows of more than one route to reach a destination network and those routes have equal metrics. EIGRP can even be configured to do load balancing across unequal-cost paths.

Different routing protocols can use different parameters in their calculation of a metric. The specific parameters used for a variety of routing protocols are presented later in this chapter.

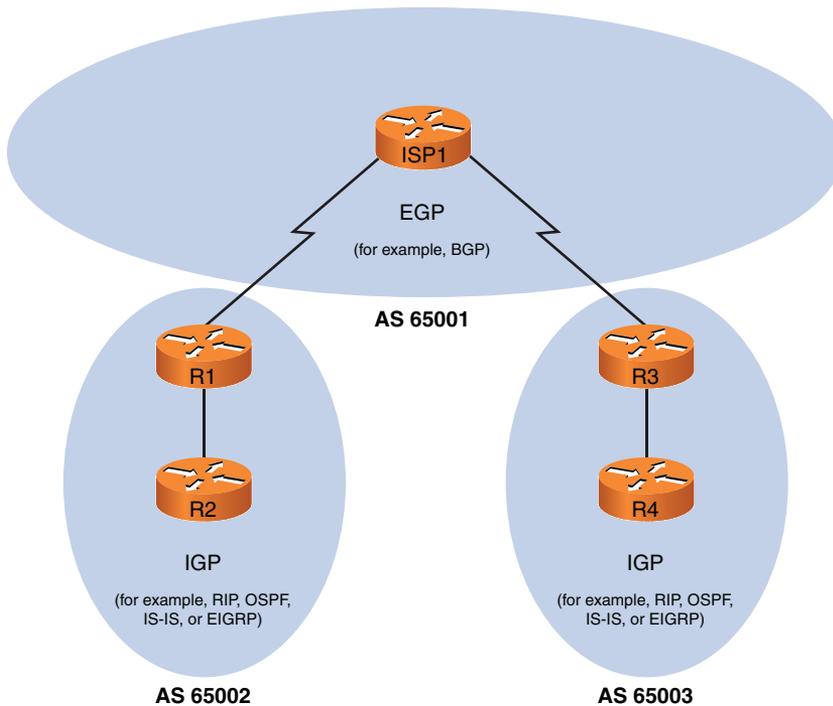
Interior Versus Exterior Gateway Protocols

Routing protocols can also be categorized based on the scope of their operation. Interior gateway protocols (IGPs) operate within an autonomous system, where an autonomous system is a network under a single administrative control. Conversely, exterior gateway protocols (EGPs) operate between autonomous systems.

Consider Figure 10-9. Routers R1 and R2 are in one autonomous system (AS 65002), and routers R3 and R4 are in another autonomous system (AS 65003). Within those autonomous systems, an IGP is used to exchange routing information. However, router ISP1 is a router in a separate autonomous system (AS 65001) that is run by a service provider. An EGP (typically, Border Gateway Protocol) is used to exchange routing information between the service provider's autonomous system and each of the other autonomous systems.

Route Advertisement Method

Another characteristic of a routing protocol is how it receives, advertises, and stores routing information. The two fundamental approaches are *distance vector* and *link state*.

**Key
Topic****FIGURE 10-9** IGPs Versus EGPs**Distance Vector**

A *distance-vector routing protocol* sends a full copy of its routing table to its directly attached neighbors. This is a periodic advertisement, meaning that even if there have been no topological changes, a distance-vector routing protocol will, at regular intervals, advertise again its full routing table to its neighbors.

Obviously, this periodic advertisement of redundant information is inefficient. Ideally, you want a full exchange of route information to occur only once and subsequent updates to be triggered by topological changes.

Another drawback to distance-vector routing protocols is the time they take to converge, which is the time required for all routers to update their routing tables in response to a topological change in a network. *Hold-down timers* can speed the convergence process. After a router makes a change to a route entry, a hold-down timer prevents any subsequent updates for a specified period of time. This approach helps stop flapping routes (which are routes that oscillate between being available and unavailable) from preventing convergence.

Yet another issue with distance-vector routing protocols is the potential of a routing loop. To illustrate, consider Figure 10-10. In this topology, the metric being used is *hop count*, which is the number of routers that must be crossed to reach a network. As one example, router R3's routing table has a route entry for network 10.1.1.0/24 available off router R1. For router R3 to reach that network, two routers must be transited (routers R2 and R1). As a result, network 10.1.1.0/24 appears in router R3's routing table with a metric (hop count) of 2.

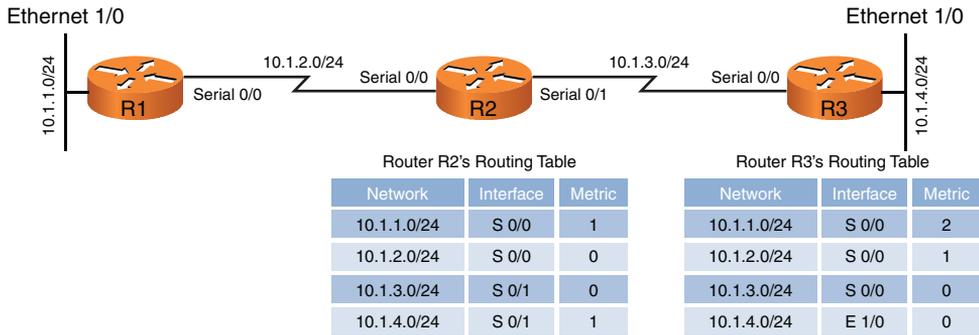


FIGURE 10-10 Routing Loop: Before Link Failure

Continuing with the example, imagine that interface Ethernet 1/0 on router R3 goes down. As shown in Figure 10-11, router R3 loses its directly connected route (with a metric of 0) to network 10.1.4.0/24. However, router R2 had a route to 10.1.4.0/24 in its routing table (with a metric of 1), and this route was advertised to router R3. Router R3 adds this entry for 10.1.4.0 to its routing table and increments the metric by 1.

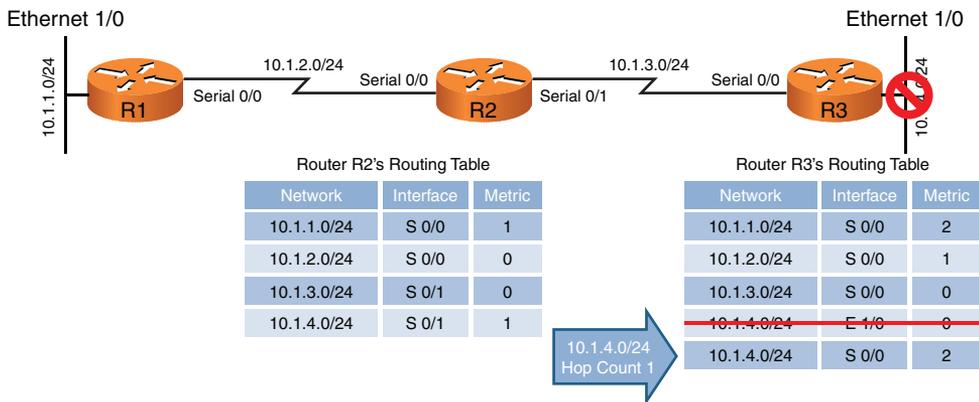


FIGURE 10-11 Routing Loop: After Link Failure

The problem with this scenario is that the 10.1.4.0/24 entry in router R2's routing table was due to an advertisement router R2 received from router R3. Now, router R3 is relying on that route, which is no longer valid. The routing loop continues as router R3 advertises its newly learned route 10.1.4.0/24 with a metric of 2 to its neighbor, router R2. Because router R2 originally learned the 10.1.4.0/24 network from router R3, when it sees router R2 advertising that same route with a metric of 2, the network gets updated in router R2's routing table to have a metric of 3, as shown in Figure 10-12.

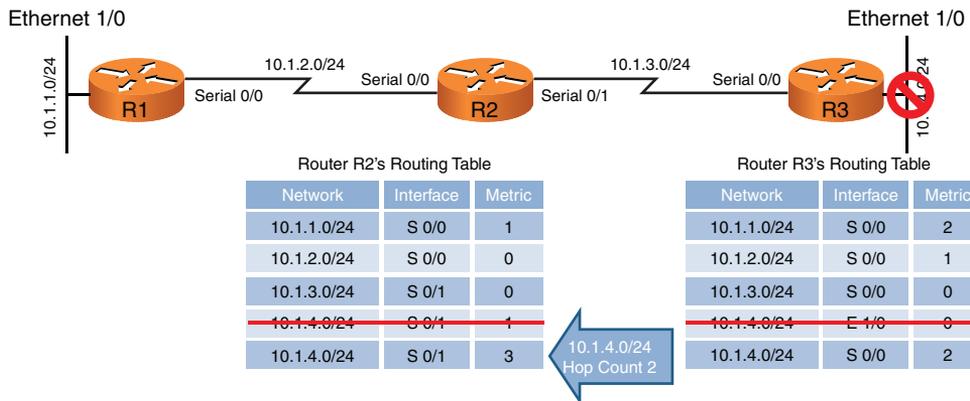


FIGURE 10-12 Routing Loop: Routers R2 and R3 Incrementing the Metric for 10.1.4.0/24

The metric for the 10.1.4.0/24 network continues to increment in the routing tables for both routers R2 and R3 until the metric reaches a value considered to be an unreachable value (for example, 16 in the case of RIP). This process is referred to as a *routing loop*.

Key Topic

Distance-vector routing protocols typically use one of two approaches for preventing routing loops:

- **Split horizon:** The split-horizon feature prevents a route learned on one interface from being advertised back out that same interface.
- **Poison reverse:** The poison-reverse feature causes a route received on one interface to be advertised back out that same interface with a metric that is considered to be infinite.

In the previous example, either approach would have prevented router R3 from adding the 10.1.4.0/24 network to its routing table based on an advertisement from router R2.

Link State

Rather than having neighboring routers exchange their full routing tables with one another, a *link-state* routing protocol allows routers to build a topological map of the network. Then, much like a Global Positioning System (GPS) device in a car, a router can execute an algorithm to calculate an optimal path (or paths) to a destination network.

Routers send *link-state advertisements (LSAs)* to advertise the networks they know how to reach. Routers then use those LSAs to construct the topological map of a network. The algorithm that runs against this topological map is *Dijkstra's shortest path first* algorithm.

Unlike distance-vector routing protocols, *link-state routing protocols* exchange full routing information only when two routers initially form their adjacency. Then routing updates are sent in response to changes in the network, as opposed to being sent periodically. Also, link-state routing protocols benefit from shorter convergence times compared to distance-vector routing protocols.

Routing Protocol Examples

Key Topic

Now that you understand some of the characteristics that distinguish one routing protocol from another, this section contrasts some of the most popular routing protocols used in modern networks:

- **Routing Information Protocol (RIP):** RIP is a distance-vector routing protocol that uses the metric *hop count*. The maximum number of hops between two routers in an RIP-based network is 15. Therefore, a hop count of 16 is considered to be infinite. Also, RIP is an IGP.
- **Open Shortest Path First (OSPF):** OSPF is a link-state routing protocol that uses the metric *cost*, which is based on the link speed between two routers. OSPF is a popular IGP because of its scalability, fast convergence, and vendor interoperability.
- **Intermediate System-to-Intermediate System (IS-IS):** This link-state routing protocol is similar in operation to OSPF. It uses a configurable, yet dimensionless, metric associated with an interface and runs Dijkstra's shortest path first algorithm. Although IS-IS is an IGP that offers the scalability, fast convergence, and vendor-interoperability benefits of OSPF, it has not been as widely deployed as OSPF.

- **Enhanced Interior Gateway Routing Protocol (EIGRP):** EIGRP is a Cisco-proprietary protocol that is popular in Cisco-only networks but less popular in mixed-vendor environments. Like OSPF, EIGRP is an IGP that offers fast convergence and scalability. EIGRP is more challenging to classify as a distance-vector or a link-state routing protocol.

By default, EIGRP uses bandwidth and delay in its metric calculation; however, other parameters can be considered, including reliability, load, and maximum transmission unit (MTU) size. Using delay as part of the metric, EIGRP can take into consideration the latency caused by the slowest links in the path.

Some literature calls EIGRP an *advanced distance-vector* routing protocol, and some literature calls it a *hybrid routing protocol* (mixing characteristics of both distance-vector and link-state routing protocols). EIGRP uses information from its neighbors to help select an optimal route (like distance-vector routing protocols). However, EIGRP also maintains a database of topological information (like a link-state routing protocol). The algorithm EIGRP uses for its route selection is not Dijkstra's shortest path first algorithm. Instead, EIGRP uses Diffusing Update Algorithm (DUAL).

- **Border Gateway Protocol (BGP):** BGP is the only EGP in widespread use today. In fact, BGP is considered to be the routing protocol that runs the Internet, which is an interconnection of multiple autonomous systems. Although some literature classifies BGP as a distance-vector routing protocol, it can more accurately be described as a *path-vector* routing protocol, meaning that it can use as its metric the number of autonomous system hops that must be transited to reach a destination network, as opposed to a number of required router hops. BGP's path selection is not solely based on autonomous system hops, however. BGP can consider a variety of other parameters. Interestingly, none of those parameters are based on link speed. In addition, although BGP is incredibly scalable, it does not quickly converge in the event of a topological change.

NOTE When studying for the Network+ exam, be sure to focus on RIP, OSPF, EIGRP, and BGP as these are the dynamic routing protocols that the exam is sure to cover.

Table 10-2 compares the key characteristics of dynamic routing protocols.

Table 10-2 Comparing Dynamic Routing Protocols

Routing Protocol	IGP or EGP	Type	Metric
RIP	IGP	Distance vector	Hop count
OSPF	IGP	Link state	Cost (based on bandwidth)
EIGRP	IGP	Hybrid	Composite (bandwidth and delay by default)
BGP	EGP	Path vector	Path attributes

A network can simultaneously support more than one routing protocol through the process of *route redistribution*. For example, a router could have one of its interfaces participating in an OSPF area of the network and have another interface participating in an EIGRP area of the network. This router could then take routes learned via OSPF and inject those routes into the EIGRP routing process. Similarly, EIGRP-learned routes could be redistributed into the OSPF routing process.

Bandwidth Management

While the main concern with routing is ensuring that data packets (as well as control plane packets) reach their rightful destinations, it is the job of *quality of service* (QoS) to ensure that packets do not suffer from long delays (latency) or, worse, dropped packets.

QoS is actually a suite of technologies that allows you to strategically optimize network performance for select traffic types. For example, in today's converged networks (that is, networks simultaneously transporting voice, video, and data), some applications (for example, voice) might be more intolerant of delay (or *latency*) than other applications; for example, an FTP file transfer is less latency sensitive than a VoIP call. Fortunately, through the use of QoS technologies, you can identify which traffic types need to be sent first, how much bandwidth to allocate to various traffic types, which traffic types should be dropped first in the event of congestion, and how to make the most efficient use of the relatively limited bandwidth of an IP WAN. This section introduces QoS and a collection of QoS mechanisms.

NOTE Do not get confused by the many uses we have for the word *converged* in networking. It all depends on the context. For example, when speaking about the network in general and what data it can carry, a converged network is one that includes multiple forms of traffic—for example VoIP and data traffic. When we are speaking of a single routing protocol—converged means the device has learned of all the updates that have been in the routing protocol's information.

Introduction to QoS

A lack of bandwidth is the overshadowing issue for most network quality problems. Specifically, when there is a lack of bandwidth, packets might suffer from one or more of the symptoms listed in Table 10-3.

Key Topic

Table 10-3 Three Categories of Quality Issues

Issue	Description
Delay	Delay is the time required for a packet to travel from source to destination. You might have witnessed delay on the evening news when the news anchor is talking via satellite to a foreign news correspondent. Because of the satellite delay, the conversation begins to feel unnatural.
Jitter	Jitter is the uneven arrival of packets. For example, imagine a VoIP conversation where packet 1 arrives at a destination router. Then, 20 ms later, packet 2 arrives. After another 70 ms, packet 3 arrives, and then packet 4 arrives 20 ms behind packet 3. This variation in arrival times (that is, <i>variable delay</i>) is not due to dropped packets, but the jitter might be interpreted by the listener as dropped packets.
Drops	Packet drops occur when a link is congested and a router's interface queue overflows. Some types of traffic, such as UDP traffic carrying voice packets, are not retransmitted if packets are dropped.

Fortunately, QoS features available on many routers and switches can recognize important traffic and then treat that traffic in a special way. For example, you might want to allocate 128Kbps of bandwidth for your VoIP traffic and give that traffic priority treatment.

Consider water flowing through a series of pipes with varying diameters. The water's flow rate through those pipes is limited to the water's flow rate through the pipe with the smallest diameter. Similarly, as a packet travels from source to destination, its effective bandwidth is the bandwidth of the slowest link along that path. For example, in Figure 10-13, notice that the slowest link speed is 256Kbps. This weakest link becomes the effective bandwidth between client and server.

Because the primary challenge of QoS is a lack of bandwidth, the logical question is, "How do we increase available bandwidth?" A knee-jerk response to that question is often "Add more bandwidth." However, more bandwidth often comes at a relatively high cost.

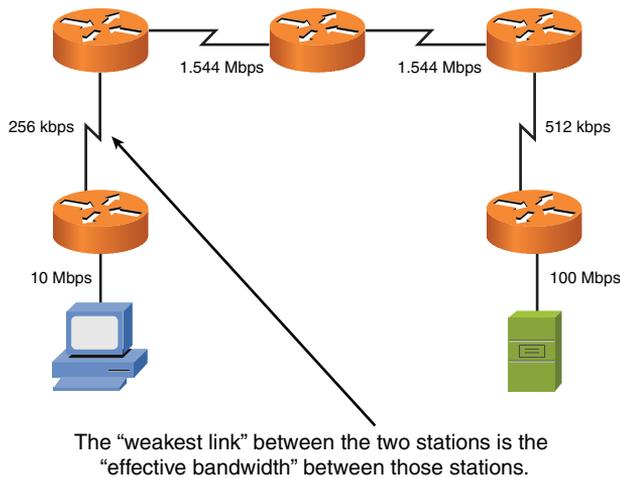


FIGURE 10-13 Effective Bandwidth of 256Kbps

Think of your network as a highway system in a large city. During rush hour, the lanes of the highway are congested; during other periods of the day, the lanes might be underutilized. Instead of just building more lanes to accommodate peak traffic rates, the highway engineers might add a carpool lane to give higher priority to cars with two or more occupants. Similarly, you can use QoS features to give your mission-critical applications higher-priority treatment in times of network congestion.

QoS Configuration Steps

The mission statement of QoS could read something like this: “To categorize traffic and apply a policy to those traffic categories, in accordance with a QoS policy.” Understanding this underlying purpose of QoS can help you better understand the three basic steps involved in QoS configuration:

Key Topic

- Step 1.** Determine network performance requirements for various traffic types. For example, consider these design recommendations for voice, video, and data traffic:
- **Voice:** No more than 150 ms of one-way delay; no more than 30 ms of jitter; and no more than 1% packet loss.
 - **Video:** No more than 150 ms of one-way delay for interactive voice applications (for example, video conferencing); no more than 30 ms of jitter; and no more than 1% of packet loss.
 - **Data:** Applications have varying delay and loss requirements. Therefore, data applications should be categorized into predefined *classes*

of traffic, where each class is configured with specific delay and loss characteristics.

- Step 2.** Categorize traffic into specific categories. For example, you might have a category named *Low Delay* for voice and video packets in that category. You might also have a *Low Priority* class for traffic such as music downloads from the Internet.
- Step 3.** Document your QoS policy and make it available to your users. Then, for example, if users complain that their network gaming applications are running slowly, you can point them to your corporate QoS policy, which describes how applications such as network gaming have *best-effort* treatment, while VoIP traffic receives *priority* treatment.

The actual implementation of these steps varies based on the specific device you are configuring. In some cases, you might be using the command-line interface (CLI) of a router or switch. In other cases, you might have some sort of graphical user interface (GUI) through which you configure QoS on your routers and switches.

QoS Components

QoS features are categorized into one of the three categories shown in Table 10-4.



Table 10-4 Three Categories of QoS Mechanisms

Issue	Description
Best effort	Best-effort treatment of traffic does not truly provide QoS to that traffic because there is no reordering of packets. Best effort uses a first-in, first-out (FIFO) queuing strategy, where packets are emptied from a queue in the same order in which they entered the queue.
Integrated Services (IntServ)	IntServ is often referred to as <i>hard QoS</i> because it can make strict bandwidth reservations. IntServ uses signaling among network devices to provide bandwidth reservations. Resource Reservation Protocol (RSVP) is an example of an IntServ approach to QoS. Because IntServ must be configured on every router along a packet's path, the main drawback of IntServ is its lack of scalability.
Differentiated Services (DiffServ)	DiffServ, as its name suggests, differentiates between multiple traffic flows. Specifically, packets are marked, and routers and switches can then make decisions (for example, dropping or forwarding decisions) based on those markings. Because DiffServ does not make an explicit reservation, it is often called <i>soft QoS</i> . Most modern QoS configurations are based on the DiffServ approach.

Figure 10-14 summarizes these three QoS categories.

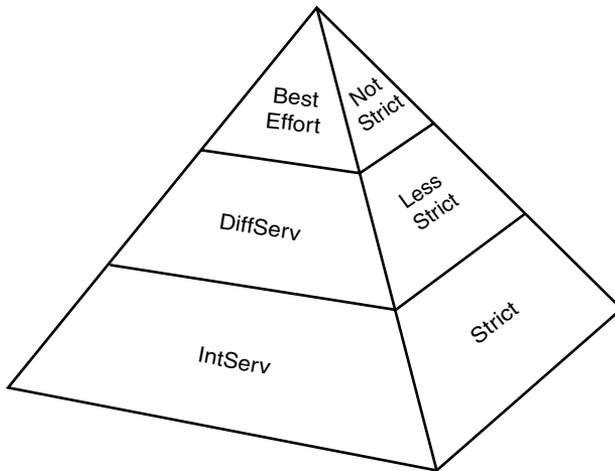


FIGURE 10-14 QoS Categories

QoS Mechanisms

As previously mentioned, a DiffServ approach to QoS marks traffic. However, for markings to impact the behavior of traffic, a QoS tool must reference those markings and alter the packets' treatment based on them. The following is a collection of commonly used QoS mechanisms:

- Classification
- Marking
- Congestion management
- Congestion avoidance
- Policing and shaping
- Link efficiency

While all of these mechanisms can be considered important, this chapter focuses on the main bandwidth management tools policing and traffic shaping.

Policing and Traffic Shaping

Key Topic

Instead of making a minimum amount of bandwidth available for specific traffic types, you might want to limit available bandwidth. Both *traffic policing* and *traffic shaping* tools can accomplish this objective. Collectively, these tools are called *traffic conditioners*.

Policing can be used in either the inbound or the outbound direction, and it typically discards packets that exceed the configured rate limit, which you can think of as a *speed limit* for specific traffic types. Because policing drops packets, resulting in retransmissions, it is recommended for higher-speed interfaces.

Shaping buffers (and therefore delays) traffic exceeding a configured rate. Therefore, shaping is recommended for slower-speed interfaces.

Because traffic shaping (and policing) can limit the speed of packets exiting a router, a question arises: “How do you send traffic out of an interface at a rate that is less than the physical clock rate of the interface?” For this to be possible, shaping and policing tools do not transmit all the time. Specifically, they send a certain number of bits or bytes at line rate, and then they stop sending until a specific timing interval (for example, one-eighth of a second) is reached. After the timing interval is reached, the interface again sends a specific amount of traffic at the line rate. It stops and waits for the next timing interval to occur. This process continually repeats, allowing an interface to send an average bandwidth that might be below the physical speed of the interface. This average bandwidth is called the *committed information rate (CIR)*. The number of bits (the unit of measure used with shaping tools) or bytes (the unit of measure used with policing tools) that is sent during a timing interval is called the *committed burst (Bc)*. The timing interval is written as T_c .

For example, imagine that you have a physical line rate of 128Kbps, but the CIR is only 64Kbps. Also, assume that there are eight timing intervals in a second (that is, $T_c = 1/8$ second = 125 ms), and during each of those timing intervals, 8000 bits (the committed burst parameter) are sent at the line rate. Therefore, over the period of a second, 8000 bits are sent (at the line rate) eight times, for a grand total of 64,000 bits per second, which is the CIR. Figure 10-15 illustrates this shaping of traffic to 64Kbps on a line with a rate of 128Kbps.

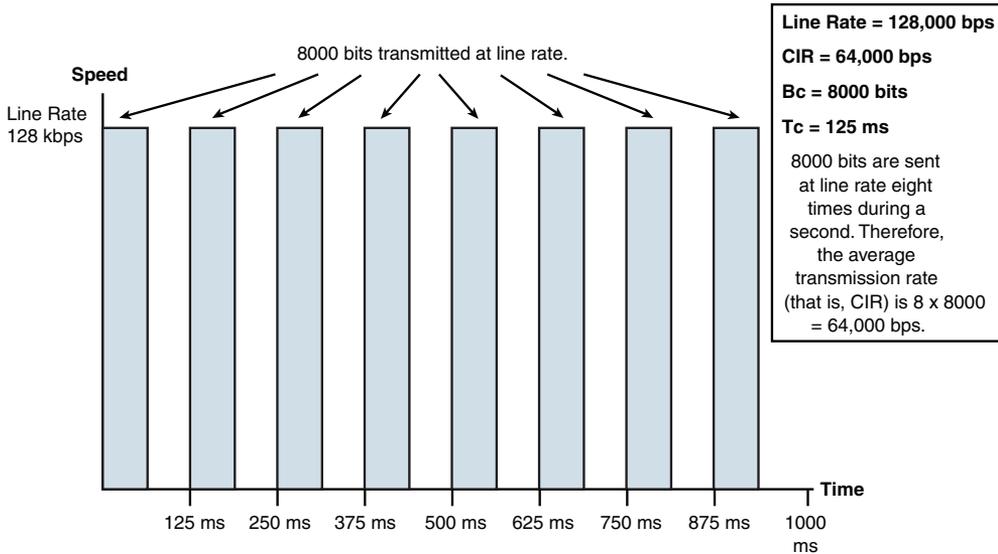


FIGURE 10-15 Traffic Shaping

If all the Bc bits (or bytes) are not sent during a timing interval, there is an option to *bank* those bits and use them during a future timing interval. The parameter that allows this storing of unused potential bandwidth is called the *excess burst* (*Be*) parameter. The Be parameter in a shaping configuration specifies the maximum number of bits or bytes that can be sent in excess of the Bc during a timing interval, if those bits are indeed available. For those bits or bytes to be available, they must have gone unused during previous timing intervals. Policing tools, however, use the Be parameter to specify the maximum number of bytes that can be sent during a timing interval. Therefore, in a policing configuration, if the Bc equals the Be, no excess bursting occurs. If excess bursting occurs, policing tools consider this excess traffic to be *exceeding traffic*. Policing tools consider traffic that conforms to (that is, does not exceed) a specified CIR to be *conforming traffic*.

The relationship between the Tc, Bc, and CIR is given with this formula: $CIR = Bc / Tc$. Alternatively, the formula can be written as $Tc = Bc / CIR$. Therefore, if you want a smaller timing interval, you can configure a smaller Bc.

Real-World Case Study

Acme, Inc. has decided to use a link-state routing protocol for dynamic routing between its LANs and the remote offices, which are connected over the WANs. The link-state protocol the company has chosen is OSPF. Each of the routers that has

connections to the LAN and WAN subnets will learn about and advertise OSPF routes with its OSPF neighbors.

The branch offices will have a default route that points toward the headquarters' routers, and at the headquarters' site, they will use a default route that points toward the service provider. Acme, Inc. itself will not be using BGP, but its WAN and Internet service provider, which is interacting with other service providers, will use BGP.

The WAN connection to one of the remote offices is very low bandwidth and is prone to becoming congested with traffic. It also occasionally drops all connection to the remote office's router. Acme, Inc., has decided to use traffic shaping as part of the QoS configuration to attempt to ensure that the link is used more sparingly and is not overwhelmed with traffic during key business hours.

Summary

Here are the main topics covered in this chapter:

- This chapter discusses how routers forward traffic through a network based on source and destination IP addresses.
- This chapter also covers the sources of route information used to populate a router's routing table. These sources include directly connected routes, statically configured routes, and dynamically learned routes.
- This chapter distinguishes between routed protocols (for example, IP) and routing protocols (such as OSPF or EIGRP).
- Some routing sources are more trustworthy than other routing sources, based on their administrative distances.
- Different routing protocols use different metrics to select the best route in the presence of multiple routes.
- This chapter distinguishes between IGPs (which run within an autonomous system) and EGPs (which run between autonomous systems).
- This chapter contrasts the behavior of distance-vector and link-state routing protocols and shows how split horizon and poison reverse can prevent routing loops in a distance-vector routing protocol environment.
- This chapter describes today's most popular routing protocols (including RIP, OSPF, IS-IS, EIGRP, and BGP), along with their characteristics.
- This chapter reviews various QoS technologies, with an emphasis on traffic shaping, which can limit the rate of data transmission on a WAN link to the CIR.

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 10-5 lists these key topics and the page number where each is found.

**Key
Topic**

Table 10-5 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
Step list	Basic routing process	256
Table 10-1	Administrative distance	263
Figure 10-9	IGPs versus EGPs	265
List	Preventing routing loops	267
List	Routing protocol examples	268
Step list	QoS configuration	272
Table 10-4	Three categories of QoS mechanisms	273
Section	Limiting available bandwidth through traffic policing and traffic-shaping tools	275

Complete Tables and Lists from Memory

Print a copy of Appendix C, “Memory Tables,” or at least the section for this chapter and complete as many of the tables as possible from memory. Appendix D, “Memory Tables Answer Key,” includes the completed tables and lists so you can check your work.

Define Key Terms

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

Address Resolution Protocol (ARP), Time-to-Live (TTL), default static route, next-hop IP address, routed protocol, routing protocol, administrative distance (AD), metric, interior gateway protocol (IGP), exterior gateway protocol (EGP), distance-vector routing protocol, link-state routing protocol, hold-down timer, split horizon, poison reverse, link-state advertisement (LSA), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior

Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), route redistribution, quality of service (QoS), traffic shaping, traffic policing, dynamic routing, hybrid routing protocol

Additional Resources

An OSPF Review: <https://www.ajsnetworking.com/an-ospf-review/>

EIGRP's Composite Metric: <https://www.ajsnetworking.com/eigrp-metric>

Review Questions

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

1. If a PC on an Ethernet network attempts to communicate with a host on a different subnet, what destination IP address and destination MAC address will be placed in the packet/frame header sent by the PC?
 - a. **Destination IP: IP address of the default gateway. Destination MAC: MAC address of the default gateway.**
 - b. **Destination IP: IP address of the remote host. Destination MAC: MAC address of the default gateway.**
 - c. **Destination IP: IP address of the remote host. Destination MAC: MAC address of the remote host.**

- d. Destination IP: IP address of the remote host. Destination MAC: MAC address of the local PC.**
2. What protocol is used to request a MAC address that corresponds to a known IPv4 address on the local network?
 - a. IGMP
 - b. TTL
 - c. ICMP
 - d. ARP
 3. What is the network address and subnet mask of a default route?
 - a. 255.255.255.255/32
 - b. 0.0.0.0/32
 - c. 255.255.255.255/0
 - d. 0.0.0.0/0
 4. What routing protocol characteristic indicates the believability of the routing protocol (compared to other routing protocols)?
 - a. Weight
 - b. Metric
 - c. Administrative distance
 - d. SPF algorithm
 5. Which of the following are distance-vector routing protocol features that can prevent routing loops? (Choose two.)
 - a. Reverse path forwarding (RPF) check
 - b. Split horizon
 - c. Poison reverse
 - d. Rendezvous point
 6. Which of the following is a distance-vector routing protocol with a maximum usable hop count of 15?
 - a. BGP
 - b. EIGRP
 - c. RIP
 - d. OSPF

7. Which of the following routing protocols is an EGP?
 - a. BGP
 - b. EIGRP
 - c. RIP
 - d. OSPF

8. What is the term for unpredictable variation in delay in a modern network?
 - a. Congestion
 - b. Contention
 - c. Jitter
 - d. Serialization delay

9. The RSVP protocol is associated with which overall approach to QoS in a modern network?
 - a. DiffServ
 - b. IntServ
 - c. FIFO
 - d. Best effort

10. What QoS tool seeks to smooth out bandwidth utilization by buffering excess packets?
 - a. Traffic policing
 - b. Traffic shaping
 - c. Weighted Random Early Detection (WRED)
 - d. Integrated Services (IntServ)

Index

Numbers

- 2G (Edge) cellular technology, 333
- 2.4GHz frequency band
 - nonoverlapping channels, 338–339
 - WLAN, 327–329
- 3DES (Triple Data Encryption Standard), 419
- 3G cellular technology, 333
- 4G cellular technology, 333
- 5G cellular technology, 333
- 5GHz frequency band, WLAN, 327, 329
- 8-bit subnet masks, 114
- 10BASE2 cable standard, 91–92
- 10BASE2 Ethernet standard, 94, 284–285, 291
- 10BASE5 cable standard, 90–92
- 10BASE5 Ethernet standard, 94, 284–285, 291
- 10BASE-T cable standard, 92–93
- 10BASE-T Ethernet standard, 94, 285–286, 291, 292
- 10GBASE-ER Ethernet standard, 94, 292
- 10GBASE-EW Ethernet standard, 94, 292
- 10GBASE-LR Ethernet standard, 94, 292
- 10GBASE-LW Ethernet standard, 94, 292
- 10GBASE-SR Ethernet standard, 94, 292
- 10GBASE-SW Ethernet standard, 94, 292
- 10GBASE-T Ethernet standard, 94, 292
- 10-Gigabit Ethernet, 93, 290
- 40 MHz mode, channel bonding, 332
- 40GBASE-SR Ethernet standard, 292
- 40GBASE-T Ethernet standard, 94
- 66 blocks, 97
- 100BASE-FX Ethernet standard, 94, 291
- 100BASE-SX Ethernet standard, 94
- 100BASE-T Ethernet standard, 95
- 100BASE-TX Ethernet standard, 94, 291, 292
- 100GBASE-ER4 Ethernet standard, 94, 292
- 100GBASE-LR4 Ethernet standard, 94, 292
- 100GBASE-SR10 Ethernet standard, 94, 292
- 100-Gigabit Ethernet, 93, 290
- 110 blocks, 98
- 802.1Q standard (dot1q), 297, 442
- 802.1X user authentication, 309–310, 430, 477
- 802.11 wireless standard, 247, 333
- 802.11a wireless standard, 331, 333
- 802.11ac (Wi-Fi 5) wireless standard, 332, 333
- 802.11ax (Wi-Fi 6) wireless standard, 327, 332, 333
- 802.11b wireless standard, 331, 333
- 802.11g wireless standard, 331, 333
- 802.11n (Wi-Fi 4) wireless standard, 332, 333
- 802.3 standard. *See* Ethernet
- 1000BASE-LH Ethernet standard, 94, 291
- 1000BASE-LX Ethernet standard, 94, 291
- 1000BASE-SX Ethernet standard, 94, 291
- 1000BASE-T Ethernet standard, 94, 291
- 1000BASE-TX Ethernet standard, 94, 95, 291
- 1000BASE-X Ethernet standard, 292
- 1000BASE-ZX Ethernet standard, 94, 292

A

- A records, DNS, 187
- AAA (Authentication, Authorization, Accounting), 477

- AAAA records, DNS, 187
- Acceptable Use Policies (AUP), 379, 382
- access
 - ACL, 457
 - Ethernet switches, 311–312
 - IoT, controlling, 459
 - LDAP, 429, 478
 - NAC, 427, 477
 - RBAC, 425–426
 - remote access, 465, 474–475
 - 802.1X user authentication, 477
 - AAA, 477
 - authentication, 478–479
 - authorization, 478–479
 - captive portals, 478
 - case studies, 480
 - CHAP, 477
 - EAP, 478
 - ICA, 476
 - IKEv2, 473
 - in-band management, 479–480
 - IPsec, AH, 470–471
 - IPsec, ESP, 470–471
 - IPsec with IKE, 468–470, 472–473
 - Kerberos, 477
 - LDAP, 478
 - local authentication, 478
 - MFA, 478
 - MS-CHAP, 478
 - NAC, 477
 - out-of-band management, 479–480
 - PPP, 476
 - PPPoE, 476
 - RADIUS, 477
 - RDC, 475
 - RDP, 475
 - remote desktop gateways, 475
 - RRAS, 475
 - SSH, 476
 - SSO, 478
 - TACACS+, 477
 - TFA, 478
 - virtual desktops, 476
 - VNC, 476
 - VPN, 466–474
 - VPN, IPsec site-to-site, 472–473
 - remote access policies, 381–382
 - role-based access, 457
 - TACACS+, 429, 477
 - access control hardware
 - badge readers, 488
 - biometrics, 488
 - access control panels (controllers), 245
 - access control vestibules (mantraps), 245, 489
 - access/edge layer, three-tiered network architectures, 198–199
 - access ports, Ethernet switches, 295
 - accounting, AAA, 477
 - ACL (Access Control Lists), 457, 564
 - action plans, troubleshooting, 500
 - active hubs, 222
 - active routers, 312
 - AD (Administrative Distance), 263
 - ad hoc WLAN, 322, 334
 - address filtering, MAC, 341
 - addressing (logical), network layer (OSI model), 15
 - ADSL (Asymmetric DSL), 62–63
 - advanced distance-vector routing protocols.
 - See* EIGRP
 - advertisements
 - LSA, 268
 - neighbors, 151
 - RA Guard, 456
 - routers, 151
 - advertising methods, routing, 264–268
 - AES (Advanced Encryption Standard), 345, 419
 - Aggressive mode, IPsec with IKE, 469
 - AH (Authentication Headers), 470–471
 - alerts
 - CRC errors, 367
 - giants, 367
 - AM (amplitude) modulation, 9
 - amplified DoS attacks, 440
 - analog phones, 245
 - analysis application, NetFlow, 368
 - analyzers
 - NetFlow analyzers, 522
 - protocol analyzers, 520–521

- spectrum analyzers, 513
- WiFi analyzers, 520
- anomaly-based detection, IDS/IPS, 242
- ANT+, 247
- antennas, 324
 - design goals, 324–325
 - gain, 325
 - omnidirectional antennas, 325–326, 551
 - placement of, 458
 - polarity, 326
 - polarization, 551
 - troubleshooting, 551
 - unidirectional antennas, 326, 551
- anycast IPv6 addresses, 153–154
- AP (Access Points), 234, 243
 - association times, 552
 - CAPWAP, 324
 - hotspots, 322
 - LWAPP, 324
 - placement, troubleshooting, 554
 - placement of, 458
 - rogue AP, 340, 443
 - TAP, 513
 - troubleshooting, 554
 - WAP, 323–324
 - interference, 552
 - placement of, 338–339
- APC (Angled Physical Contact), fiber-optic cable, 90
- API (Application Programming Interface), northbound/southbound operations, 201–202
- APIPA (Automatic Private IP Addressing), 116, 128–129
- application layer
 - OSI model, 21–22
 - application services, 22
 - service advertisements, 22
 - SDN, 201
 - TCP/IP stack, 25
- application logs, 363
- application protocols, TCP/IP stack, 26–27
- application services, application layer (OSI model), 22
- architectures, network, 197
 - case studies, 206
 - collapsed core design, 200
 - deciding on, 205–206
 - SAN, 204
 - FCoE, 205
 - Fibre Channel, 204
 - IB, 205
 - iSCSI, 205
 - SDN, 200–201, 202
 - application layer, 201
 - control layer, 201–202
 - infrastructure layer, 202
 - management layer, 202
 - spine and leaf topologies, 202–204
 - three-tiered network architectures, 198
 - access/edge layer, 198–199
 - core layer, 200
 - distribution/aggregation layer, 199–200
- ARIN (American Registry for Internet Numbers), 115
- ARP (Address Resolution Protocol)
 - DAI, 456
 - requests, 225–231, 256–257
 - spoofing, 442
 - VLAN, 293
- arp command, 533–535
- ARPANET, NCP, 22
- assessments
 - business risk assessments, 432–433
 - posture assessments, 432
 - process assessments, 432–433
 - reports, 387
 - threat assessments, 431
 - vendor assessments, 433
 - vulnerability assessments, 432
- asset disposal, 489
 - factory resets, 489
 - HIPAA, 490
 - legislation, 490
 - sanitizing devices for disposal, 489
 - wipe configurations, 489
- asset tracking tags, 486
- assigning
 - dynamic addresses, DHCP, 182
 - IP addresses, 118–119, 130

- BOOTP, 126, 128
- DHCP, 126–128
 - dynamic IP configurations, 126–128
 - static IP configurations, 120–125
- static addresses, DHCP, 182
- VLAN, troubleshooting, 563
- association times, AP, 552
- associations, WLAN, 323
- asymmetric encryption, 420–422
- asymmetrical routing, troubleshooting, 565
- asynchronous synchronization, 10
- asynchronous transmissions, LLC, 14
- attacks
 - ARP spoofing, 442
 - botnets, 441
 - brute-force password attacks, 443
 - buffer overflows, 448
 - case studies, 449
 - command and control software, 441
 - confidentiality attacks, 446
 - data diddling, 447
 - DDoS attacks, 441
 - deauthentication attacks, 444
 - dictionary password attacks, 443
 - DNS poisoning, 442
 - DoS attacks, 440–441
 - dumpster diving, 446
 - electrical disturbances, 448
 - EMI interception, 446
 - environmental-based attacks, 445
 - evil twins (rogue AP), 443
 - FTP bounce, 447
 - human-based attacks, 445
 - ICMP attacks, 448
 - information sent over covert channels, 447
 - information sent over overt channels, 446
 - IP spoofing, 444
 - logic bombs, 448
 - MAC spoofing, 444
 - malware, 444–445
 - Man-in-the-Middle (MitM) attacks.
 - See* on-path attacks
 - on-path attacks, 441
 - packet capturing, 446
 - packet sniffing, 446
 - password attacks, 443
 - phishing, 445
 - piggybacking, 445
 - ping of death, 448
 - ping sweeps, 446
 - port scanning, 446
 - ransomware, 443
 - reconnaissance attacks, 446
 - rogue AP, 443
 - salami attacks, 447
 - scanning attacks, 446
 - session hijacking, 447
 - shoulder surfing, 445
 - Smurf attacks, 448
 - SYN flooding, 448
 - tailgating, 445
 - TCP flooding, 448
 - technology-based attacks, 440–445
 - trust relationship exploitation, 448
 - VLAN hopping, 442
 - wiretapping, 446
 - zero-day attacks, 424
 - zombies, 441
- attenuation
 - troubleshooting, 507
 - WLAN, 550
- audit and assessment reports, 387
- audit logs, 361
- AUP (Acceptable Use Policies), 379, 382
- authentication, 428
 - 802.1X user authentication, 342–343, 430, 477
 - AAA, 477
 - CHAP, 477
 - deauthentication attacks, 444
 - EAP, 343, 431, 458, 478
 - Ethernet switches, 311–312
 - Kerberos, 429–430, 477
 - LDAP, 429
 - local authentication, 430, 478
 - MFA, 428, 478
 - open authentication, WLAN, 341
 - RADIUS, 342
 - RADIUS, 429, 477
 - remote access, 478–479

- servers, 477
- SNMP security, 359
- SSO, 429, 478
- TACACS+, 429
- TFA, 478
- WLAN, open authentication, 341
- authentication servers, 802.1X user
 - authentication, 310, 430
- authenticators, 310, 430, 477
- authNoPriv, 358
- authoritative domain servers, 187
- authorization
 - AAA, 477
 - remote access, 478–479
- authPriv, 358
- automation
 - defined, 214
 - Obtain a DNS address automatically, 184
 - Obtain an IP address automatically, 184–185
- availability, CIA, 423, 468
- availability, network (uptime)
 - case studies, 368, 410–411
 - content caching, 401
 - environmental monitors, 354, 365
 - HA, 394
 - backups, 400
 - best practices, 400–401
 - design considerations, 399–400
 - fault-tolerant network design, 395–396
 - hardware redundancy, 397
 - Layer 3 redundancy, 398–399
 - measuring, 394
 - MTBF, 394
 - MTTF, 394
 - MTTR, 394
 - RPO, 395
 - RTO, 395
 - SLA, 394
 - hardware redundancy, 402–403
 - interface statistics/statuses, 367
 - CRC, 367
 - encapsulation errors, 367
 - giants, 367
 - link-state, 366
 - packet byte counts, 367
 - protocol byte counts, 367
 - send/receive traffic, 366
 - speed/duplex, 366
 - viewing, 365–366
 - load balancing, 401–402
 - logs, 363
 - application logs, 363
 - audit logs, 361
 - Event Viewer logs, 360
 - reviews, 360
 - security logs, 364
 - syslog, 361–363
 - system logs, 364
 - traffic logs, 360
 - NetFlow, 368
 - performance metrics, 354
 - bandwidth, 355
 - baselines, 356
 - CPU usage, 354
 - jitter, 355
 - latency (delay), 355
 - memory, 355
 - temperature, 354
 - SNMP, 356
 - community strings, 357–358
 - Get messages, 357
 - MIB, 356–357
 - OID, 357
 - security, authentication, 359
 - security, authNoPriv, 358
 - security, authPriv, 358
 - security, encryption, 359
 - security, integrity, 359
 - security, levels, 358
 - security, models, 358
 - security, noAuthNoPriv, 358
 - Set messages, 357
 - SNMP agent, 356
 - SNMP manager, 356
 - SNMPv1, 357–358, 359
 - SNMPv2c, 357–358, 359
 - SNMPv3, 358–360
 - Trap messages, 357
 - walks, 357

- SOHO network design, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
 - available hosts, calculating number of, 134
 - available leases, DHCP, 184
 - avoiding collisions, 288
- B**
- back-off timers, Ethernet collisions, 287
 - back-out plans, 500
 - backups, 400
 - differential backups, 400
 - full backups, 400
 - incremental backups, 400
 - snapshots, 400
 - bad cable, troubleshooting, 508
 - bad ports, troubleshooting, 508
 - badge readers, 245, 488
 - balancing loads, 401–402
 - bandwidth
 - Ethernet, 93–94, 290–291
 - managing. *See* QoS
 - Mbps, 93
 - network availability, 355
 - physical layer (OSI model), 10
 - baseband technologies, 10
 - broadband technologies, 10, 11
 - QoS, 270–272
 - best-effort treatment, 273
 - categories, 274
 - $CIR = Bc / Tc$ formula, 276
 - components of, 273–274
 - configuring, 272–273
 - conforming traffic, 276
 - data, 272–273
 - delay (latency), 270, 271, 273
 - DiffServ, 273
 - drops, packets, 271
 - exceeding traffic, 276
 - IntServ, 273
 - jitter, 271
 - mechanisms, 274–276
 - policing traffic, 275–276
 - priority treatment, 273
 - shaping traffic, 275–276
 - soft QoS, 273
 - $Tc = Bc / CIR$ formula, 276
 - video, 272
 - voice, 272
 - speed testers, 520
 - baseband technologies, physical layer (OSI model), 10
 - baselines
 - configurations, 387
 - network availability, 356
 - network configuration/performance baselines, 387
 - BCP (Business Continuity Plans), 377
 - behavior-based detection. *See* anomaly-based detection, IDS/IPS
 - believability of routes, 263
 - best practices
 - HA, 400–401
 - hardening networks, 454–457
 - best-effort treatment
 - QoS, 273
 - traffic, 273
 - BGP (Border Gateway Protocol), 269, 270
 - binary numbering, 106
 - ARIN, 115
 - converting
 - conversion table, 106
 - to decimal numbers, 107
 - decimal numbers to, 107–109
 - practice exercises, 109–112
 - IANA, 116
 - ICANN, 115
 - principles of, 106

- biometrics, security, 488
- bit splitters (hubs), 222–223, 234, 242, 243
- BIX (Building Industry Cross-Connect)
 - blocks, 98
- block size, 137
- blocked IP addresses, troubleshooting, 564
- blocked services, troubleshooting, 564
- blocked TCP/UDP ports, troubleshooting, 564
- Bluetooth, 247, 345
- BNC connectors, 81
- bonding
 - channels, 332
 - NIC, 397
- bookshelf, OSI reference model as, 4–5
- BOOTP (Bootstrap Protocol), 126, 128, 182
- borrowed bits, classful masks, 133
- botnets, 441
- bottom-to-top troubleshooting, 499
- bridges, 223–225, 234, 242
 - nonroot bridges, 301
 - root bridges, 301
- Bring Your Own Device (BYOD) policies, 382, 566
- broadband technologies, physical layer (OSI model), 10
- broadcast domains, 117, 234
 - Layer 2 switches, 230–231
 - switching, 293
- broadcast frames, flooding, 224
- broadcast IP addresses, 117
- broadcast storms, 300–301, 565
- broadcasts, 341
- brute-force password attacks, 443
- BSS WAN, 334, 335
- buffer overflows, 448
- buffering, transport layer (OSI model), 18
- bus topologies, 46–48, 286
- Business Continuity Plans (DRP), 377
- business risk assessments, 432–433
- BYOD (Bring Your Own Device) policies, 382, 566
- byte counts, protocols/packets, 367
- bytes, port tagging, 297

C

- CA (Certificate Authorities), 421
- cabinets, locking, 245, 488
- cable crimpers, 509–510
- cable modems, 64–65, 235–236, 243
- cable strippers, 514
- cable testers, 513
- cabling
 - 10BASE2 cable standard, 91–92
 - 10BASE5 cable standard, 90–92
 - 10BASE-T cable standard, 92–93
 - 66 blocks, 97–98
 - 110 blocks, 98
 - BIX, 98
 - BNC connectors, 81
 - case studies, 99, 514
 - Cat 5 cable, 83
 - Cat 5e cable, 84
 - Cat 6 cable, 84
 - Cat 6a cable, 84
 - Cat 7 cable, 84
 - Cat 8 cable, 84
 - coaxial cable, 80
 - 10BASE2 cable standard, 91–92
 - BNC connectors, 81
 - EMI, 80
 - F-connectors, 81
 - RFI, 80
 - RG-6 coaxial cables, 81
 - RG-58 coaxial cables, 81
 - RG-59 coaxial cables, 80
 - twinaxial cables, 81
 - console cable, 507
 - crimpers, 509–510
 - cross-connect blocks, 97–98
 - crossover cable, 85, 297, 507
 - cutters/snips, 513
 - distance (signal), 506
 - distribution systems, 97
 - EMI, 80
 - Ethernet
 - crossover cable, pin mappings, 85
 - networks, 290
 - standards, 90–93
 - types of (overview), 94–95

- F-connectors, 81
- fiber distribution panels, 96
- fiber light meters, 514
- fiber-optic cable, 86–87
 - APC, 90
 - cladding, 87
 - fiber connector polishing styles, 90
 - fiber distribution panels, 96
 - LC, 90–91
 - light propagation, 87–89
 - low optical link budgets,
 - troubleshooting, 566
 - MMF, 89, 94
 - mode of propagation, 87, 89
 - MTRJ, 90–91
 - multimode delay distortion, 89
 - multimode fiber-optic cable, 87–89
 - multiplexing, 95–96
 - PC, 90
 - refractive index, 87
 - SC, 90–91
 - SMF cable, 89, 94
 - ST connectors, 89
 - standards, 90–93
 - UPC, 90
- fire codes, 507
- fusion splicers, 513
- IDE, 96
- Krone (Krone LSA-PLUS) blocks, 98
- limitations, 506
- loopback plugs, 510–511
- managing, 96–99
- MDF, 98
- media converters, 99
- multimeters, 512–513
- nonplenum cable, 86
- OTDR, 511–512
- patch bays, 96
- patch panels, 96
- plenum cable, 86, 506–507
- PoE, 507
- punchdown blocks, 96
- punchdown tools, 509
- reflectometers, 511–512
- RFI, 80
- riser rated cabling, 507
- rollover cable, 507
- snips/cutters, 513
- specifications, 506
- spectrum analyzers, 513
- speed (data rates), 506
- STP cable, 506
- strippers, 514
- TAP, 513
- TDR, 511–512
- testers, 513
- throughput, 506
- tone generators, 510
- tools, 509–514
- troubleshooting, 507
 - attenuation, 507
 - bad cable, 508
 - bad ports, 508
 - decibel (dB) loss, 508
 - dirty optical cables, 509
 - duplexing, 509
 - interference, 508
 - LED status indicators, 508
 - opens, 508
 - pinouts, 508
 - pins, 508
 - receive (Rx) reads, 509
 - shorts, 508
 - speed (data rates), 509
 - transceivers, 508
 - transmit (Tx) reads, 509
- twisted-pair cable, 82
 - DB-9 (RS-232) connectors, 85–86
 - RJ11 connectors, 85–86
 - RJ45 connectors, 85–86
 - STP cable, 82–83, 506
 - TIA/EIA-568 standard, 82
 - UTP cable, 83–85, 92–93, 506
- UTP cable, 285–286, 506
- wire maps, 513
- wiring closets, 96
- wiring diagrams, 386
- caching content, 401
- calculating
 - CIDR, 144

- IP address ranges, 137–139
 - number of available hosts, 134
 - number of subnets, 133
- call agents, 245
- cameras, 246, 486
- CAN (Campus Area Networks), 39
- captive portals, 459, 478, 554
- capturing packets, 307–309, 446, 520–521
- CAPWAP (Control and Provisioning of Wireless Access Points), 324
- cards, smart, 488
- CARP (Common Address Redundancy Protocol), 313, 398
- case studies
 - architectures, network, 206
 - attacks, 449
 - availability, network, 368
 - cabling, 99, 514
 - cloud computing, 217
 - command line tools, 543
 - corporate architectures, 206
 - datacenter architectures, 206
 - disaster recovery, 410–411
 - documentation, 387–388
 - Ethernet switches, 314–315
 - IP addressing, 154
 - monitoring, 368
 - network availability, 368, 410–411
 - network devices, 248–249
 - network hardening, 459
 - network platform commands, 543
 - network services, 191
 - network topologies, 69
 - network troubleshooting, 566–567
 - organizational documents/policies, 387–388
 - physical security, 490
 - plans/policies, 387–388
 - reference models, 27–28
 - remote access, 480
 - routing, 276–277
 - security, 434–459
 - software tools, 543
 - SOHO network design, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
 - troubleshooting, 501, 556
 - wireless standards, 345–346
 - WLAN, 345–346, 556
- Cat 5 cable, 83
- Cat 5e cable, 84
- Cat 6 cable, 84
- Cat 6a cable, 84
- Cat 7 cable, 84
- Cat 8 cable, 84
- CCTV cameras, 246
- CDMA (Code-Division Multiple Access), 334
- CE (Customer Edge) routers, 41
- cells, WLAN, 338
- cellular technologies, 333–334
- center frequency, 330
- Certificate Authorities (CA), 421
- change management plans, 376, 386
- channels, 327
 - bonding, 332
 - center frequency, 330
 - honeycomb channels, 339
 - nonoverlapping channels, 328, 338–339
 - overlaps, 555
 - troubleshooting, 552
 - wireless channels, 327
 - WLAN, 327–329
- CHAP (Challenge-Handshake Authentication Protocol), 477
- cheapernet, 91, 284
- child tunnels, 473
- CIA (Confidentiality, Integrity, Availability), 418
 - availability, 423
 - confidentiality, 418–419

- asymmetric encryption, 420–422
 - symmetric encryption, 419–420, 422
- integrity, 422–423
- IPsec with IKE, 468
- CIDR (Classless Interdomain Routing), 144
- $CIR = Bc / Tc$ formula, 276
- circuit switching, network layer (OSI model), 15
- circuits
 - E1 circuits, 66–67
 - E3 circuits, 67
 - T1 circuits, 66
 - T3 circuits, 67
- cladding, fiber-optic cable, 87
- classful masks, 115
 - borrowed bits, 133
 - CIDR, 144
 - extending, 132–133
- classifying NAT IP addresses, 146–147
- client disassociation issues, troubleshooting, 554
- clientless VPN, 468
- clients
 - NTP, 190
 - syslog, 361
 - wireless client isolation, 458
- client/server networks, 42–43
- client-to-site VPN, 466
- cloud computing
 - automation, 214
 - case studies, 217
 - community clouds, 212, 213
 - connectivity, 215
 - DaaS, 213
 - deployments, 212–213
 - elasticity, 215–216
 - hybrid clouds, 212, 213
 - IaaS, 213
 - IaC, 214
 - multitenancy, 215
 - orchestration, 214
 - PaaS, 213
 - private clouds, 212
 - public clouds, 212
 - SaaS, 213
 - scalability, 216
 - security, 216
 - services, 213
 - VPN, 215
 - XaaS, 213
- cloud sites, 403
- clustering, 397
- CNAME records, DNS, 187
- coaxial cable, 80
 - 10BASE2 cable standard, 91–92
 - BNC connectors, 81
 - EMI, 80
 - F-connectors, 81
 - RFI, 80
 - RG-6 coaxial cables, 81
 - RG-58 coaxial cables, 81
 - RG-59 coaxial cables, 80
 - twinaxial cables, 81
- cold sites, 402
- collapsed core design, 200
- collectors, 522
- collision domains, 222, 234
- collisions
 - avoidance, 288
 - CSMA/CA, 288
 - CSMA/CD, 288–290
 - domains, 288–289
 - Ethernet, 286–287
 - Layer 2 switches, 230–231
 - troubleshooting, 565
- command and control software, 441
- command line tools, 522, 537
 - arp command, 533–535
 - case studies, 543
 - dig command, 531–532
 - ifconfig command, 528–529
 - ip command, 529
 - ipconfig command, 524–528
 - ipconfig/all command, 526–527
 - ipconfig/release command, 527–528
 - netstat command, 535–537
 - nmap command, 542
 - nslookup [fqdn] command, 529–531
 - nslookup command, 529, 531
 - ping command, 523–524
 - route add command, 541–542

- route command, 538–542
- route delete command, 540–541
- route print command, 538–540
- tcpdump command, 542
- traceroute command, 532–533
- common passwords/usernames, 454
- Common Vulnerability Scoring System (CVSS), 424
- community clouds, 212, 213
- community strings, 357–358
- computer clusters, 397
- concentrators, VPN, 236–237, 243
- confidentiality attacks, 446
- confidentiality, CIA, 418–419
 - asymmetric encryption, 420–422
 - IPsec with IKE, 468
 - symmetric encryption, 419–420, 422
- configuring
 - baselines, 387
 - IP addresses
 - BOOTP, 126, 128
 - DHCP, 126–128
 - dynamic IP configurations, 126–128
 - static IP configurations, 120–125
 - network configuration/performance
 - baselines, 387
 - network devices, troubleshooting, 562
 - NTP, 190
 - QoS, 272–273
 - VPN
 - full tunnel configurations, 468
 - split tunnel configurations, 468
 - wipe configurations, 489
- conforming traffic, 276
- congestion control. *See* flow control
- connection services
 - LLC, 13
 - network layer (OSI model), 16
- connectionless communications, 172
- connection-oriented communications, 172
- connectivity, cloud computing, 215
- connectors
 - BNC connectors, 81
 - DB-9 (RS-232) connectors, 85–86
 - Ethernet connectors, 291
 - F-connectors, 81
 - fiber connector polishing styles, 90
 - LC, 90–91
 - RJ11 connectors, 85–86
 - RJ45 connectors, 9, 85–86
 - SC, 90–91
 - ST connectors, 89
 - T connectors, 46–47
 - wiring standards, 9
- console cable, 507
- content caching, 401
- content engines, 401
- content switching, 401–402
- control layer, SDN, 201–202
- Control Plane Policing (CoPP), 456
- controllers (access control panels), 245
- converters, media, 99
- converting
 - binary numbers
 - conversion table, 106
 - to decimal numbers, 107
 - practice exercises, 109–112
 - decimal numbers to binary numbers, 107–109
- CoPP (Control Plane Policing), 456
- cordless phones, RFI, 337
- core layer, three-tiered network architectures, 200
- corporate architectures, 197
 - case studies, 206
 - collapsed core design, 200
 - deciding on, 205–206
 - SAN, 204
 - FCoE, 205
 - Fibre Channel, 204
 - IB, 205
 - iSCSI, 205
 - SDN, 200–201, 202
 - application layer, 201
 - control layer, 201–202
 - infrastructure layer, 202
 - management layer, 202
 - spine and leaf topologies, 202–204
 - three-tiered network architectures, 198
 - access/edge layer, 198–199

- core layer, 200
- distribution/aggregation layer, 199–200
- cost savings, SOHO network design, 409
- covert channels, information sent over, 447
- CPE (Customer Premises Equipment), 41
- CPU usage, network availability, 354
- CRAM-MD5 (Challenge-Response Authentication Mechanism-Message Digest 5), 423
- CRC (Cyclic Redundancy Checks), 14, 367
- credentials
 - default credentials, changing, 454
 - new credentials, generating, 455
- crimpers, 509–510
- cross-connect blocks, 66 blocks, 97
- crossover cable, 297, 507
- CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance), 288, 329
- CSMA/CD (Carrier-Sense Multiple Access with Collision Detection), 288–290
- current state modulation, 8
- cutters/snips, 513
- CVSS (Common Vulnerability Scoring System), 424
- CWDM (Coarse Wavelength-Division Multiplexing), 68, 96

D

- DaaS (Desktop as a Service), 213
- DAI (Dynamic ARP Inspection), 456
- data diddling, 447
- Data Encryption Standard (DES), 419
- data formatting, presentation layer (OSI model), 21
- data link layer (OSI model), 11
 - DLC, 12
 - LLC, 13–14
 - MAC, 12–13
 - MTU, 11, 12
 - NIC, 14
- Data Loss Prevention (DLP) policies, 380–381
- data, QoS, 272–273
- data rates (speed)
 - bandwidth speed testers, 520
 - cabling, 506, 509
 - WLAN, troubleshooting, 550
- datacenter architectures, 197
 - case studies, 206
 - collapsed core design, 200
 - deciding on, 205–206
 - SAN, 204
 - FCoE, 205
 - Fibre Channel, 204
 - IB, 205
 - iSCSI, 205
 - SDN, 200–201, 202
 - application layer, 201
 - control layer, 201–202
 - infrastructure layer, 202
 - management layer, 202
 - spine and leaf topologies, 202–204
 - three-tiered network architectures, 198
 - access/edge layer, 198–199
 - core layer, 200
 - distribution/aggregation layer, 199–200
- DB-9 (RS-232) connectors, 85–86
- dBi, gain, 325
- DDNS (Dynamic DNS), 188
- DDoS (Distributed Denial-of-Service) attacks, 441
- deauthentication attacks, 444
- decapsulation, 28
- decibel (dB) loss, troubleshooting, 508
- decimal numbers, converting
 - binary numbers to, 107
 - practice exercises, 109–112
 - to binary numbers, 107–109
- default credentials, changing, 454
- default gateways, 119, 312
- default static routes, 260
- default VLAN, changing, 457
- defense-in-depth security, 426
 - honeynets, 428
 - honeypots, 428
 - NAC, 427
 - network segmentation enforcement, 427
 - screened subnets, 427
 - separation of duties, 427
- delay (latency), 270, 271

- Low Delay, voice/video, 273
- network availability, 355
- satellite provider links, 61
- troubleshooting, 553
- variable delay, 271
- demarcation points, 55
- Denial-of-Service (DoS) attacks, 440–441
- deployments
 - cloud computing, 212–213
 - WLAN, 334–339
- DES (Data Encryption Standard), 419
- design considerations, HA, 399–400
- designated ports, STP, 302
- designing SOHO networks, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
- desktops
 - remote desktops
 - gateways, 475
 - RDC, 475
 - RDP, 475
 - virtual desktops, 58–60, 476
- detection methods, 486
 - asset tracking tags, 486
 - cameras, 486
 - IDS/IPS
 - anomaly-based detection, 242
 - policy-based detection, 241
 - signature-based detection, 241
 - motion detection, 486
 - tamper detection, 486
- devices, network, 221–222
 - AP, 234, 243
 - bridges, 223–225, 234, 242
 - broadcast domains, 293
 - BYOD policies, 382, 566
 - cameras, 246
 - case studies, 248–249
 - configurations, troubleshooting, 562
 - encryption devices, 237
 - firewalls, 238, 243
 - full-duplex mode, 289
 - half-duplex mode, 289
 - hubs, 222–223, 234, 242, 243
 - HVAC sensors, 246
 - ICS, 248
 - IDS, 239, 243
 - anomaly-based detection, 242
 - categories, 241–242
 - IPS versus, 239–240
 - network placement, 239–240
 - policy-based detection, 241
 - signature-based detection, 241
 - IoT technologies, 246–247
 - IPS, 239
 - anomaly-based detection, 242
 - categories, 241–242
 - IDS versus, 239–240
 - network placement, 239–240
 - policy-based detection, 241
 - signature-based detection, 241
 - Layer 2 switches, 225–231, 234, 243
 - Layer 3 capable switches, 231–232, 234, 243
 - load balancers, 235, 243
 - media converters, 243
 - modems
 - cable modems, 235–236, 243
 - DSL modems, 235, 243
 - multilayer switches, 231–232, 234, 243
 - network addresses, 293
 - physical access control, 245–246
 - printers, 245
 - proxy servers, 237–238
 - routers, 233, 234, 243
 - SCADA, 248
 - VoIP devices/protocols, 244–245
 - VPN concentrators, 236–237, 243
 - VPN headends, 236–237

- WAP, 234
 - wireless security system devices, RFI, 337
- WLC, 235, 243
- DHCP (Dynamic Host Configuration Protocol), 166, 170, 175, 182
 - DHCPv6, 151
 - DORA acronym, 184
 - dynamic address assignment, 182
 - IP addressing, 126–128, 182–183
 - IP helpers/DHCP relays, 183–184
 - leases, 184
 - Obtain a DNS address automatically, 184
 - Obtain an IP address automatically, 184–185
 - relay agents, 183–184
 - reservations, 184
 - rogue DHCP servers, 442, 564
 - scope, 184
 - scope exhaustion, troubleshooting, 564
 - snooping, 456
 - static address assignment, 182
 - diagnosing problems, 497
 - diagnostics, Ethernet switches, 313–314
 - diagram symbols, 386
 - dictionary password attacks, 443
 - diddling, data, 447
 - differential backups, 400
 - DiffServ (Differentiated Services), 273
 - dig command, 531–532
 - Dijkstra's shortest path first algorithm, 268
 - directed broadcast addresses, 117
 - directly connected routes, 259
 - directories, LDAP, 429, 478
 - dirty optical cables, troubleshooting, 509
 - disabling
 - SSID broadcasts, 341
 - unnneeded network services, 455
 - unnneeded switch ports, 455
 - disassociation, clients, 554
 - disaster recovery
 - case studies, 410–411
 - content caching, 401
 - fault-tolerant network design, 395
 - no single point of failure, 396
 - single points of failure, 395–396
- HA
 - backups, 400
 - best practices, 400–401
 - design considerations, 399–400
 - fault-tolerant network design, 395–396
 - hardware redundancy, 397
 - Layer 3 redundancy, 398–399
 - measuring, 394
 - MTBF, 394
 - MTTF, 394
 - MTTR, 394
 - RPO, 395
 - RTO, 395
 - SLA, 394
 - hardware redundancy, 402–403
 - load balancing, 401–402
 - SOHO network design, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
- Disaster Recovery Plans (DRP), 377
- disposing of assets, 489
 - factory resets, 489
 - HIPAA, 490
 - legislation, 490
 - sanitizing devices for disposal, 489
 - wipe configurations, 489
- distance (attenuation), WLAN,
 - troubleshooting, 550
- distance (signal), cabling, 506
- distance-vector routing protocols, 265–267.
 - See also* EIGRP
- Distributed Denial-of-Service (DDoS)
 - attacks, 441

- distribution systems, cabling, 97
- distribution/aggregation layer, three-tiered
 - network architectures, 199–200
- divide-and-conquer troubleshooting, 499
- DLC (Data Link Control), 12
- DLP (Data Loss Prevention) policies, 380–381
- DMVPN (Dynamic Multipoint VPN), mGRE, 41
- DMZ (Demilitarized Zones). *See* screened subnets
- DNAT (Dynamic NAT), 147
- DNS (Domain Name Systems), 166, 170, 175
 - DNS TTL, 189
 - forward lookups, 189
 - FQDN, 185–186, 189
 - global DNS systems, 189
 - global hierarchy, 186–187
 - iterative lookups, 190
 - mDNS, 129
 - Obtain a DNS address automatically, 184
 - poisoning, 442
 - recursive lookups, 190
 - reverse lookups, 189
 - servers, 185–186
 - A records, 187
 - AAAA records, 187
 - authoritative domain servers, 187
 - CNAME records, 187
 - DDNS, 188
 - EDNS, 188
 - external DNS servers, 187
 - internal DNS servers, 187
 - IP addressing, 188
 - IPAM, 188
 - MX records, 187
 - NS records, 187
 - PTR records, 188
 - record types (overview), 187–188
 - root DNS servers, 187
 - SOA records, 188
 - SRV records, 188
 - TXT records, 188
 - URL, 189
 - zone transfers, 189
- DOCSIS (Data Over Cable Service Interface Specification), 65
 - documents/policies, 375–376
 - audit and assessment reports, 387
 - AUP, 379, 382
 - baseline configurations, 387
 - BCP, 377
 - BYOD policies, 382
 - case studies, 387–388
 - change management plans, 376, 386
 - diagram symbols, 386
 - DLP policies, 380–381
 - DRP, 377
 - fair use policies, 382
 - floor plans, 386
 - hardening/security policies, 378–380
 - IDF documentation, 386
 - incident response plans, 376–377
 - international export controls, 385
 - inventory management, 387
 - labeling, 386
 - licensing restrictions, 384
 - logical network diagrams, 386
 - MDF documentation, 386
 - MOU, 387
 - NDA, 385
 - network configuration/performance
 - baselines, 387
 - onboarding/offboarding procedures, 384
 - password policies, 378–379
 - physical network diagrams, 385, 386
 - port location diagrams, 386
 - PUA, 383
 - rack diagrams, 386
 - remote access policies, 381–382
 - safety procedure policies, 383
 - site surveys, 387, 552
 - SLA, 387, 394
 - SOP, 386
 - system life cycles, 377–378
 - wiring diagrams, 386
 - work instructions, 386
- DoD model. *See* TCP/IP stack
- domains, collision, 288–289
- door switches, magnetic, 246

- DORA acronym, 184
 - DoS (Denial-of-Service) attacks, 440–441
 - dot1q, 297, 442
 - dotted-decimal notation, IPv4 addresses, 113
 - downstream data frequencies, 65
 - downtime, hot sites, 402
 - drops, packets, 271
 - DRP (Disaster Recovery Plans), 377
 - DS3 (Digital Signal 3), 67
 - DSL (Digital Subscriber Line), 62
 - ADSL, 62–63
 - modems, 235, 243
 - SDSL, 63
 - VDSL, 64
 - DSo (Digital Signature o), 65
 - DSSS (Direct-Sequence Spread Spectrum), 330
 - DUAL (Diffusing Update Algorithm), 269
 - dual power supplies, 400
 - dual stacks, 149
 - dumpster diving, 446
 - duplexing
 - speed/duplex statistics/statuses, 366
 - troubleshooting, 509
 - duplicate IP addresses, troubleshooting, 563
 - duplicate MAC addresses, troubleshooting, 563
 - duties, separation of, 427
 - DWDM (Dense Wavelength-Division Multiplexing), 68, 96
 - dynamic address assignment, DHCP, 182
 - dynamic IP configurations, 126–128
 - dynamic routing, 259, 261–262
- E**
- E1 circuits, 66–67
 - E3 circuits, 67
 - EAP (Extensible Authentication Protocol), 343, 431, 458, 478
 - east-west traffic flows, 201–202
 - ECMP (Equal-Cost Multipathing), 396
 - EDNS (Extension Mechanisms for DNS), 188
 - EGP (Exterior Gateway Protocols), 263, 264–265
 - EIGRP (Enhanced Interior Gateway Routing Protocol), 268–269, 270, 396. *See also* distance-vector routing protocols
 - EIRP (Effective Isotropic Radiated Power), WLAN, troubleshooting, 551
 - elasticity, cloud computing, 215–216
 - electrical disturbances, 448
 - ELSR (Edge Label Switch Routers), 41
 - emanations, EMI, 446
 - EMI (Electromagnetic Interference), 80
 - EMI interception, 446
 - employees, training, prevention methods, 486–487
 - emulators, terminal, 522
 - encapsulation errors, 367
 - encryption, 419
 - 3DES, 419
 - AES, 345, 419
 - asymmetric encryption, 420–422
 - DES, 419
 - devices, 237
 - GPG, 420
 - PGP, 420
 - presentation layer (OSI model), 21
 - RC4 encryption, 343–344
 - SNMP security, 359
 - symmetric encryption, 419–420, 422
 - end-of-chapter review tools, exam preparation, 573
 - end-of-rack switching, 204
 - Enterprise mode, WPA2, 345
 - entry points, service-related, 55
 - environmental factors, SOHO network design, 409
 - environmental monitors, 354, 365
 - environmental-based attacks
 - phishing, 445
 - piggybacking, 445
 - shoulder surfing, 445
 - tailgating, 445
 - ephemeral ports, 27
 - error control, LLC, 13
 - errors
 - CRC, 367
 - encapsulation errors, 367

- escalating issues (troubleshooting), 500
- ESF (Extended Super Frame), 66
- ESP (Encapsulating Security Payloads), 470–471
- ESS WLAN, 334
- ESSID (Extended SSID), 341
- EtherChannel, 305
- Ethernet
 - 10BASE2 Ethernet standard, 94, 284–285, 291
 - 10BASE5 Ethernet standard, 94, 291
 - 10BASE-T Ethernet standard, 94, 285–286, 291–292
 - 10GBASE-ER Ethernet standard, 94, 292
 - 10GBASE-EW Ethernet standard, 94, 292
 - 10GBASE-LR Ethernet standard, 94, 292
 - 10GBASE-LW Ethernet standard, 94, 292
 - 10GBASE-SR Ethernet standard, 94, 284–285, 292
 - 10GBASE-SW Ethernet standard, 94, 292
 - 10GBASE-T Ethernet standard, 94, 292
 - 10-Gigabit Ethernet, 93, 290
 - 40GBASE-SR Ethernet standard, 292
 - 40GBASE-T Ethernet standard, 94
 - 100BASE-FX Ethernet standard, 94, 291
 - 100BASE-SX Ethernet standard, 94
 - 100BASE-T Ethernet standard, 95
 - 100BASE-TX Ethernet standard, 94, 291, 292
 - 100GBASE-ER4 Ethernet standard, 94, 292
 - 100GBASE-LR4 Ethernet standard, 94, 292
 - 100GBASE-SR10 Ethernet standard, 94, 292
 - 100-Gigabit Ethernet, 93, 290
 - 1000BASE-LH Ethernet standard, 94, 291
 - 1000BASE-LX Ethernet standard, 94, 291
 - 1000BASE-SX Ethernet standard, 94, 291
 - 1000BASE-T Ethernet standard, 94, 291
 - 1000BASE-TX Ethernet standard, 94–95, 291
 - 1000BASE-X Ethernet standard, 292
 - 1000BASE-ZX Ethernet standard, 94, 292
 - back-off timers, 287
 - bandwidth, 290–291
 - bandwidth capacities, 93–94
 - bridges, 223–225, 234, 242
 - bus topologies, 286
 - cable standards, 90–93
 - cabling, 290
 - cheapernet, 284
 - collisions, 286–287
 - connectors, 291
 - crossover cable, 85, 297
 - CSMA/CA, 288
 - CSMA/CD, 288–290
 - Fast Ethernet, 93, 290
 - FCoE, 205
 - flow control, 290
 - GBIC, 291
 - Gigabit Ethernet, 93, 290
 - hubs, 222–223, 234, 242, 243, 288–289
 - jumbo frames, 290
 - Layer 2 switches, 225–231, 234, 243
 - MDIX, 509
 - mini-GBIC, 291
 - multilayer switches, 231–232, 234, 243
 - origins of, 284–286
 - PoE, 306–307, 507
 - PPPoE, 476
 - principles of, 284
 - SFP, 291
 - Standard Ethernet, 93, 290
 - standards (overview), 291–292
 - switches, 292
 - 802.1Q standard (dot1q), 297
 - 802.1X user authentication, 309–310
 - access management, 311–312
 - access ports, 295
 - authentication, 311–312
 - broadcast storms, 300–301
 - case studies, 314–315
 - collision domains, 289
 - connectors, 291
 - diagnostics, 313–314
 - first-hop redundancy, 312–313
 - link aggregation, 304–305
 - MAC address table corruption, 299
 - packet capturing, 307–309

- PoE, 306–307
 - PoE+, 307
 - port mirroring, 307–309
 - port monitoring, 307–309
 - port tagging, 297
 - QoS, 314
 - RSTP, 298
 - Shortest Path Bridging, 299
 - STP, 298–299, 301–303
 - subnets, 293
 - trunks, 296–297
 - VLAN, 293–295
 - thicknet, 284
 - thinnet, 284
 - Token Ring topologies, 286
 - transceivers, 95, 291
 - types of (overview), 94–95, 291–292
 - Xerox Corporation, 284
- EUI-64 (Extended Unique Identifier-64), 150, 151
- Euro-DOCSIS, 65
- Event Viewer logs, 360
- events, SEM, 433
- evil twins (rogue AP), 340–341, 443
- exams, final preparation, 577
 - end-of-chapter review tools, 573
 - exam taking strategies, 576–577
 - final review/study plan, 574–575
 - memory tables, 572–573
 - simulations/performance-based exercises, 573
 - tools, 571–572
 - video training, 572
- exceeding traffic, 276
- expired IP addresses, troubleshooting, 564
- explicit deny, 457
- exploits, 424
- export controls, international, 385
- Extensible Authentication Protocol (EAP), 431
- external DNS servers, 187
- F**
- factory resets, 489
- failures
 - fault-tolerant network design, 395–396
 - hardware, troubleshooting, 566
 - no single point of failure, 396
 - single points of failure, 395–396
 - troubleshooting
 - hardware, 566
 - MTBF, 394
 - MTTF, 394
- fair use policies, 382
- Fast Ethernet, 93, 290
- faults, network, 394
- fault-tolerant network design, 395
 - no single point of failure, 396
 - single points of failure, 395–396
- FCoE (Fiber Channel over Ethernet), 205
- F-connectors, 81
- FDM (Frequency-Division Multiplexing), physical layer (OSI model), 11
- FHRP (First Hop Redundancy Protocol), 398
- FHSS (Frequency-Hopping Spread Spectrum), 330
- fiber distribution panels, 96
- fiber light meters, 514
- fiber-optic cable, 86–87
 - APC, 90
 - cladding, 87
 - fiber connector polishing styles, 90
 - fiber distribution panels, 96
 - LC, 90–91
 - light propagation, 87–89
 - low optical link budgets, troubleshooting, 566
 - MMF, 89, 94
 - mode of propagation, 87, 89
 - MTRJ, 90–91
 - multimode delay distortion, 89
 - multimode fiber-optic cable, 87–89
 - multiplexing, 95–96
 - PC, 90
 - refractive index, 87
 - SC, 90–91
 - SMF cable, 89, 94
 - ST connectors, 89
 - standards, 90–93
 - UPC, 90

- Fibre Channel, 57, 204
 - Field of Dreams*, 36, 393
 - file servers, 36
 - filtering MAC addresses, 341, 458
 - final preparation, 577
 - end-of-chapter review tools, 573
 - exam taking strategies, 576–577
 - final review/study plan, 574–575
 - memory tables, 572–573
 - simulations/performance-based exercises, 573
 - tools, 571–572
 - video training, 572
 - final review/study plan
 - exam preparation, 574–575
 - flash card mode, 575
 - practice exam mode, 574
 - study mode, 574
 - fire codes, cabling, 507
 - fire suppression systems, SOHO network design, 409
 - firewalls, 238, 243
 - explicit deny, 457
 - implicit deny, 457
 - rules, 457
 - troubleshooting, 564
 - virtual firewalls, 58
 - firmware, upgrading, 454–455
 - first-hop redundancy, Ethernet switches, 312–313
 - flash card mode, final review/study plan, 575
 - flooding
 - broadcast frames, 224
 - multicast, troubleshooting, 565
 - SYN, 448
 - TCP, 448
 - floor plans, 386
 - flow collectors, NetFlow, 368
 - flow control
 - Ethernet, 290
 - LLC, 13
 - network layer (OSI model), 16
 - flow exporters, NetFlow, 368
 - FM (frequency) modulation, 9
 - formatting data, presentation layer (OSI model), 21
 - forward lookups, 189
 - FQDN (Fully Qualified Domain Names), DNS, 185–186, 189
 - frames
 - broadcast frames, flooding, 224
 - ESF, 66
 - IDF, 96, 386
 - jumbo frames, 57, 205, 290
 - MDF, 98
 - MDF documentation, 386
 - SE, 66
 - frequencies
 - 2.4GHz frequency band, 327–329, 338–339
 - 5GHz frequency band, 327, 329
 - center frequency, 330
 - FHSS, 330
 - heat maps, 327
 - ISM bands, 327
 - RFI, WLAN, 336–337
 - RFID, 247
 - roaming, 338
 - troubleshooting, 552
 - WLAN, 327–329
 - FTP (File Transfer Protocol), 166, 170, 174, 447
 - full backups, 400
 - full-duplex mode, network devices, 289
 - full-mesh topologies, 52–53
 - full system functionality, verifying, 500
 - full tunnel VPN configurations, 468
 - fusion splicers, 513
- ## G
- gain, antennas, 325
 - gateways
 - default gateways, 119, 312
 - GLBP, 313
 - remote desktop gateways, 475
 - voice gateways, 244
 - VoIP, 245
 - GBIC (Gigabit Interface Converters), 291
 - generators, 400
 - geofencing, 345, 459

- Get messages, 357
 - giants, 367
 - Gigabit Ethernet, 93, 290
 - GLBP (Gateway Load Balancing Protocol), 313, 399
 - global DNS systems, 189
 - global hierarchy, DNS, 186–187
 - global routing tables, 427
 - GNU Privacy Guard (GPG), 420
 - goodput, 337
 - GPG (GNU Privacy Guard), 420
 - GRE (Generic Routing Encapsulation), 173
 - mGRE, 41
 - tunneling, 471
 - GSM (Global System for Mobile Communication), 334
 - guest network isolation, 458
- H**
- H.323, 166, 170
 - HA (High Availability), 394
 - backups, 400
 - best practices, 400–401
 - design considerations, 399–400
 - fault-tolerant network design, 395
 - no single point of failure, 396
 - single points of failure, 395–396
 - hardware redundancy, 397
 - Layer 3 redundancy, 398–399
 - measuring, 394
 - MTBF, 394
 - MTTF, 394
 - MTTR, 394
 - RPO, 395
 - RTO, 395
 - SLA, 394
 - half-duplex mode, network devices, 289
 - hardening networks, 453
 - ACL, 457
 - antenna placement, 458
 - AP, 458
 - best practices, 454–457
 - captive portals, 459
 - case studies, 459
 - common passwords/usernames, 454
 - CoPP, 456
 - credentials (default), changing, 454
 - DAI, 456
 - default VLAN, changing, 457
 - DHCP snooping, 456
 - EAP, 458
 - firewall rules, 457
 - geofencing, 459
 - guest network isolation, 458
 - IoT, 458–459
 - keys/credentials (new), generating, 455
 - MAC filtering, 458
 - NIST Digital Identity Guidelines, 454
 - patches, 454
 - policies, 378–380
 - ports
 - security, 456
 - unnneeded switch ports, disabling, 455
 - power levels, adjusting, 458
 - PSK rotation, 458
 - RA Guard, 456
 - role-based access, 457
 - secure protocols, 455
 - SNMP, 455
 - STP, 456
 - updating, 454
 - upgrading, firmware, 454–455
 - VLAN
 - private VLAN, 456
 - segmentation, 456
 - wireless client isolation, 458
 - wireless security, 458–459
 - hardware
 - access control hardware
 - badge readers, 488
 - biometrics, 488
 - failures, troubleshooting, 566
 - redundancy, 397, 402–403
 - hashing, 422–423
 - HDLC (High-Level Data Link Control), 66
 - headends, VPN, 236–237
 - heat maps, 327
 - HFC (Hybrid Fiber-Coax) networks, 64
 - hierarchical structure, DNS, 186–187
 - High Availability. *See* HA

- hijacking sessions, 447
 - HIPAA, asset disposal, 490
 - hold-down timers, 265
 - honeycomb channels, 339
 - honeynets, 428
 - honeypots, 428
 - hop counts, 262, 266
 - hopping, VLAN, 442
 - hostname command, 537
 - hosts, calculating number of available, 134
 - hot sites, 402–403
 - hotspots, 322
 - HSPA+ (Evolved High-Speed Packet Access), 333
 - HSRP (Hot Standby Router Protocol), 312–313, 398
 - HT (High Throughput), 802.11n HT, 332
 - HTTP (HyperText Transfer Protocol), 26, 166, 170, 174
 - HTTPS (HTTP Secure), 26, 167, 170, 174
 - hub sites, 51
 - hub-and-spoke topologies, 51–52
 - hubs, 11, 222–223, 234, 242, 243, 288–289
 - human-based attacks
 - phishing, 445
 - piggybacking, 445
 - shoulder surfing, 445
 - tailgating, 445
 - HVAC (Heating, Ventilation, Air Conditioning)
 - sensors, 246
 - SOHO network design, 409
 - hybrid clouds, 212, 213
 - hybrid networks, 45, 54
 - hybrid routing protocols. *See* EIGRP
- I**
- IaaS (Infrastructure as a Service), 213
 - IaC (Infrastructure as Code), 214
 - IANA (Internet Assigned Numbers Authority), 116
 - IB (InfiniBand), 57, 205
 - IBSS WLAN, 322, 334
 - ICA (Independent Computer Architecture), 476
 - ICANN (Internet Corporation for Assigned Names and Numbers), 115
 - ICMP (Internet Control Message Protocol), 173, 174
 - attacks, 448
 - transport layer (OSI model), 19
 - ICS (Industrial Control Systems), 248
 - identification, RFID, 247
 - identifying problems, 499
 - IDF (Intermediate Distribution Frames), 96, 386
 - IDS (Intrusion Detection Systems), 239, 243
 - anomaly-based detection, 242
 - categories, 241–242
 - IPS versus, 239–240
 - network placement, 239–240
 - policy-based detection, 241
 - signature-based detection, 241
 - IEEE (Institute of Electrical and Electronics Engineers), 37
 - 802.1Q standard (dot1q), 297
 - 802.1X user authentication, 342–343, 477
 - 802.3 standard. *See* Ethernet
 - wireless standards, 332
 - ifconfig command, 528–529
 - IGMP (Internet Group Management Protocol), 175
 - IGP (Interior Gateway Protocols), 263, 264–265
 - IIS (Internet Information Services), 56
 - IKE (Internet Key Exchange), 468–470
 - IKEv2, 473
 - IPsec site-to-site VPN setup/tear down, 472–473
 - IMAP (Internet Message Access Protocol), 167, 170
 - IMAP over SSL, 167, 170
 - IMAP4 (Internet Message Access Protocol version 4), 174
 - implementing solutions (troubleshooting), 500
 - implicit deny, 457
 - in-band management, 479–480
 - incident response plans, 376–377
 - incorrect time, troubleshooting, 564
 - incremental backups, 400

- Independent Computer Architecture (ICA), 476
- information sent over
 - covert channels, 447
 - overt channels, 446
- infrastructure layer, SDN, 202
- infrastructure mode, WLAN, 335
- initiators, 57, 205, 469
- integrity
 - CIA, 422–423, 468
 - SNMP security, 359
- interface statistics/statuses, 367
 - CRC, 367
 - encapsulation errors, 367
 - link-state, 366
 - packet byte counts, 367
 - protocol byte counts, 367
 - send/receive traffic, 366
 - speed/duplex, 366
 - troubleshooting, 562–563
 - viewing, 365–366
- interference
 - troubleshooting, 508, 553
 - WAP, 552
 - WLAN, 336–337
- internal DNS servers, 187
- international export controls, 385
- Internet layer, TCP/IP stack, 23
- InterNIC (Internet Network Information Center), 116
- IntServ (Integrated Services), 273
- inventory management, 387
- IoT (Internet of Things) technologies, 345
 - 802.11 wireless standard, 247
 - access, controlling, 459
 - ANT+, 247
 - Bluetooth, 247
 - IR, 247
 - network devices, 246–247
 - NFC, 247
 - security, 458–459
 - Z-Wave, 247
- IP (Internet Protocol) addressing, 105, 173
 - APIPA, 116, 128–129
 - ARIN, 115
 - assigning, 130
 - binary numbering, 106
 - conversion table, 106
 - converting, practice exercises, 109–112
 - converting decimal numbers to, 107–109
 - converting to decimal numbers, 107
 - principles of, 106
 - broadcast IP addresses, 117
 - calculating, new IP address ranges, 137–139
 - case studies, 154
 - CIDR, 144
 - classful masks
 - borrowed bits, 133
 - extending, 132–133
 - decimal numbers
 - converting, practice exercises, 109–112
 - converting binary numbers to, 107
 - converting to binary numbers, 107–109
 - DHCP
 - dynamic address assignment, 182
 - static address assignment, 182
 - directed broadcast addresses, 117
 - DNS records, 188
 - dual stacks, 149
 - duplicate IP addresses, troubleshooting, 563
 - dynamic address assignment, DHCP, 182
 - expired IP addresses, troubleshooting, 564
 - IANA, 116
 - ICANN, 115
 - IPAM, 188
 - IPv4 addresses, 112
 - APIPA, 128–129
 - assigning, 118–119, 130
 - assigning, BOOTP, 126, 128
 - assigning, DHCP, 126–128
 - assigning, dynamic IP configurations, 126–128
 - assigning, static IP configurations, 120–125
 - BOOTP, 126, 128
 - broadcast IP addresses, 117
 - calculating network addresses, 114
 - calculating new IP address ranges, 137–139

- calculating number of available hosts, 134
- calculating number of subnets, 133
- classes, 114–116
- classful masks, 115, 132–133
- classifying NAT IP addresses, 146–147
- components of, 119–120
- default gateways, 119
- DHCP, 126–128
- directed broadcast addresses, 117
- dividing into network/host portions, 114
- dotted-decimal notation, 113
- dual stacks, 149
- dynamic IP configurations, 126–128
- managing IP addresses, 143
- multicast IP addresses, 118
- NAT, 145–147
- octets, 113
- packets, 23
- PAT, 147–148
- prefix (slash) notation, 114
- private IP addresses, 145
- private IP networks, 116
- ranges, 139
- RARP, 128
- static IP configurations, 120–125
- structure of, 113–114
- subinterfaces, 120
- subnet masks, 113, 114–116
- subnetting, 129–132
- subnetting, advanced practice exercises, 139–143
- subnetting, CIDR, 144
- subnetting, practice exercises, 134–136
- UNC, 119
- unicast IP addresses, 116–117
- VIP addresses, 120
- IPv6 addresses, 149
 - anycast IPv6 addresses, 153–154
 - data flows, 151–154
 - DHCPv6, 151
 - dual stacks, 149
 - EUI-64, 150, 151
 - multicast IPv6 addresses, 152–153
 - NDP, 151
 - need for, 149
 - ping command, 524
 - shorthand notation, 150
 - SLAAC, 151
 - structure of, 150
 - traceroute command, 533
 - tunneling, 149
 - types of (overview), 150–151
 - unicast IPv6 addresses, 152
- link-local IP addresses, 129
- loopback addresses, 115
- managing, 143
- mDNS, 129
- multicast IP addresses, 118
- NAT, 145–147
- next-hop IP addresses, 260
- Obtain an IP address automatically, 184–185
- PAT, 147–148
- port numbers, TCP/IP stack, 26–27
- private IP addresses, 145
- private IP networks, 116
- protocols
 - GRE, 173
 - ICMP, 173, 174
 - IPsec, 173
 - TCP, 172, 174
 - UDP, 172, 174
- ranges, 139
- RARP, 128
- scanners, 521, 522
- SOHO network design, 405–406
- spoofing, 444
- static address assignment, DHCP, 182
- subinterfaces, 120
- subnetting, 129
 - advanced practice exercises, 139–143
 - calculating new IP address ranges, 139
 - calculating number of available hosts, 134
 - calculating number of subnets, 133
 - CIDR, 144
 - managing, 143
 - practice exercises, 134–136
 - purpose of, 129–130
 - subet mask notation, 130–132
 - VLSM, 130

- troubleshooting, blocked addresses, 564
- TTL, 257–258
- UNC, 119
- unicast IP addresses, 116–117
- VIP addresses, 120
- VLSM, 130
- Zeroconf, 129
- IP cameras (netcams), 246
- ip command, 529
- IP helpers/DHCP relays, 183–184
- IP phones, 244
- IP routing tables, 259
- IP scanners, 521, 522
- IPAM (IP Address Management), 188
- ipconfig command, 524–528
- ipconfig/all command, 526–527
- ipconfig/release command, 527–528
- iperf, 521–522
- IPS (Intrusion Prevention Systems), 239, 243
 - anomaly-based detection, 242
 - categories, 241–242
 - IDS versus, 239–240
 - network placement, 239–240
 - policy-based detection, 241
 - signature-based detection, 241
- IPsec (IP Security), 173
 - AH, 470–471
 - IKE, 468–470
 - IKEv2, 473
 - IPsec site-to-site VPN setup/tear down, 472–473
 - tunneling, 470
- IR (Infrared), 247, 345
- ISAKMP (Internet Security Association and Key Management Protocol), 469–470
- iSCSI (IP-based Small Computer System Interface), 57
 - initiators, 205
 - jumbo frames, 205
 - SAN, 205
- IS-IS (Intermediate System-to-Intermediate System), 268
- ISM bands, 327
- isolation
 - guest networks, 458

- wireless clients, 458
- isynchronous transmissions, LLC, 13
- iterative lookups, 190

J

- jacks
 - MTRJ, 90–91
 - wiring standards, 9
- jitter, 271, 355
- jumbo frames, 57, 205, 290

K

- Kerberos, 429–430, 477
- key fobs, security, 488
- keys
 - IKE, 468–470
 - IKEv2, 473
 - IPsec site-to-site VPN setup/tear down, 472–473
 - ISAKMP, 469–470
 - new keys/credentials, generating, 455
- Krone (Krone LSA-PLUS) blocks, 98

L

- L2F (Layer 2 Forwarding), 474
- L2TP (Layer 2 Tunneling Protocol), 474
- label switching, 40
- labeling, 386
- LACP (Link Aggregation Control Protocol), 305, 399
- LAG (Link Aggregation Groups), 305
- LAN (Local Area Networks)
 - AP, 234, 243
 - bridges, 223–225
 - sample topology, 37–38
 - WLAN, 321–322
 - 802.11 wireless standard, 333
 - 802.11a wireless standard, 331, 333
 - 802.11ac (Wi-Fi 5) wireless standard, 332, 333
 - 802.11ax (Wi-Fi 6) wireless standard, 332, 333
 - 802.11b wireless standard, 331, 333
 - 802.11g wireless standard, 331, 333

- 802.11n (Wi-Fi 4) wireless standard, 332, 333
- ad hoc WLAN, 322, 334
- antennas, 324–326
- associations, 323
- BSS WAN, 334, 335
- case studies, 345–346
- cells, 338
- cellular technologies, 333–334
- channels, 327–329
- channels, honeycomb, 339
- channels, nonoverlapping, 338–339
- components of, 322
- concepts, 322
- CSMA/CA, 329
- deploying, 334–339
- ESS WLAN, 334
- frequencies, 327–329
- frequencies, nonoverlapping channels, 338–339
- honeycomb channels, 339
- hotspots, 322
- IBSS WLAN, 322, 334
- infrastructure mode, 335
- interference, 336–337
- mesh topology, 336
- nonoverlapping channels, 338–339
- RFI, 336–337
- security, 339–345
- transmission methods, 330–331
- WAP, 323–324, 338–339
- wireless routers, 322–323
- WLC, 324
- WLC, 235, 243
- latency (delay), 270, 271
 - Low Delay, voice/video, 273
 - network availability, 355
 - satellite provider links, 61
 - troubleshooting, 553
 - variable delay, 271
- Layer 1 media, SOHO network design, 406–407
- Layer 2 devices, SOHO network design, 407–408
- Layer 2 loops, STP, 301
- Layer 2 switches, 225–231, 234, 243
- Layer 3 capable switches, 231–232, 234, 243
- Layer 3 devices, SOHO network design, 408
- Layer 3 redundancy, 398–399
- Layer 3 to Layer 2 mapping, 259
- LC (Lucent Connectors), 90–91
- LDAP (Lightweight Directory Access Protocol), 167, 170, 175, 429, 478
- LDAPS (LDAP over SSL), 167, 171
- leased lines, 65
 - DSO, 65
 - E1 circuits, 66–67
 - E3 circuits, 67
 - HDLC, 66
 - PPP, 65
 - T1 circuits, 66
 - T3 circuits, 67
- leases, DHCP, 184
- least privilege, 425
- LED status indicators, troubleshooting, 508
- legislation, asset disposal, 490
- licensed features, troubleshooting, 566
- licensing restrictions, 384
- light meters, fiber, 514
- light propagation
 - multimode fiber-optic cable, 87–89
 - SMF cable, 89
- limitations, cabling, 506
- link-local IP addresses, 129
- links
 - aggregation, 304–305, 407
 - LACP, 399
 - LLC, data link layer (OSI model), 13–14
- link-state routing protocols, 268
- link-state statistics/statuses, 366
- LLC (Logical Link Control)
 - connection services, 13
 - data link layer (OSI model), 13–14
 - error control, 13
 - flow control, 13
 - synchronizing transmissions, 13–14
- load balancing, 235, 243, 313, 401–402
- local authentication, 430, 478
- locating network services, 129
- lockers, smart, 488

- locking cabinets, 245, 488
- locking racks, 245, 488
- locks, 245, 488
- logic bombs, 448
- logical addressing, network layer (OSI model), 15
- logical network diagrams, 386
- logical topologies
 - MAC, 13
 - physical topologies versus, 45–46
- logs, 363
 - application logs, 363
 - audit logs, 361
 - Event Viewer logs, 360
 - managing, 433
 - message structure, 362
 - reviews, 360
 - security logs, 364
 - syslog, 361
 - clients, 361
 - security, 361–362
 - system logs, 364
 - traffic logs, 360
- long STP, 303
- lookups
 - forward lookups, 189
 - iterative lookups, 190
 - recursive lookups, 190
 - reverse lookups, 189
- loopback addresses, 115
- loopback plugs, 510–511
- loops
 - Layer 2 loops, STP, 301
 - routing loops, 266–267, 565
 - switching loops, 565
- loss budgets, troubleshooting, 566
- Low Delay, voice/video, 273
- low optical link budgets, troubleshooting, 566
- Low Priority traffic, 273
- LSA (Link-State Advertisements), 268
- LSR (Label Switch Routers), 41
- LTE (Long-Term Evolution), 333
- LWAPP (Lightweight Access Point Protocol), 324

M

- MAC (Media Access Control)
 - address filtering, 341
 - address table corruption, 299
 - data link layer (OSI model), 12–13
 - duplicate MAC addresses, troubleshooting, 563
 - filtering, 458
 - logical topologies, 13
 - media transmission methods, 13
 - physical addressing, 12
 - spoofing, 444
- magnetic door switches, 246
- Main mode, IPsec with IKE, 469
- malware, 444–445
- MAN (Metropolitan Area Networks), 39
- Managed Security Service (MSS), 433
- Managed Security Service Providers (MSSP), 433
- management layer, SDN, 202
- managing
 - bandwidth. *See* QoS
 - cabling, 96–99
 - Ethernet switches
 - access management, 311–312
 - authentication, 311–312
 - in-band management, 479–480
 - inventory, 387
 - IP addressing, 143
 - logs, 433
 - out-of-band management, 479–480
 - risk, 431
 - business risk assessments, 432–433
 - penetration testing, 432
 - posture assessments, 432
 - process assessments, 432–433
 - threat assessments, 431
 - vendor assessments, 431
 - vulnerability assessments, 432
- Man-in-the-Middle (MitM) attacks.
 - See* on-path attacks
- mantraps, 245, 489
- maps
 - Layer 3 to Layer 2 mapping, 259
 - wire maps, 513

- Mbps (Megabits Per Second), 93
- MD5 (Message Digest 5), 422
- MDF (Main Distribution Frames), 98, 386
- MDI (Media-Dependent Interface), 85
- MDIX (MDI Crossover), 85, 509
- MDI-X technology, 297
- mDNS (Multicast Domain Name Systems), 129
- Mean Time Between Failures (MTBF), 394
- Mean Time To Failure (MTTF), 394
- Mean Time To Repair (MTTR), 394
- measuring HA, 394
- media converters, 99, 243
- media transmission methods, MAC, 13
- Memorandum of Understanding (MOU), 387
- memory, network availability, 355
- memory tables, exam preparation, 572–573
- mesh topology, WLAN, 336
- messages
 - SNMP
 - Get messages, 357
 - Set messages, 357
 - Trap messages, 357
 - switching, network layer (OSI model), 16
 - syslog, 362
- metrics, routing protocols, 263, 264
- metro-optical, 67
- MFA (Multifactor Authentication), 428, 478
- MGCP (Media Gateway Control Protocol), 167, 171
- mGRE (Multipoint Generic Routing Encapsulation), 41
- MIB (Management Information Base), 356–357
- MIC (Message Integrity Checks), 344
- microwave ovens, RFI, 337
- MIMO (Multiple Input, Multiple Output), 332
- mini-GBIC, Ethernet, 291
- mirroring ports, Ethernet switches, 307–309
- missing routes, troubleshooting, 566
- MitM (Man-in-the-Middle) attacks.
 - See on-path attacks
- MMF (Multimode Fiber), 89, 94
- mode of propagation
 - multimode fiber-optic cable, 87
 - SMF cable, 89
- modems
 - cable modems, 64–65, 235–236, 243
 - DSL modems, 235, 243
- modulation
 - AM modulation, 9
 - current state modulation, 8
 - FM modulation, 9
 - state transition modulation, 8–9
- monitoring
 - case studies, 368
 - environmental monitors, 354, 365
 - interface statistics/statuses, 367
 - CRC, 367
 - encapsulation errors, 367
 - giants, 367
 - link-state, 366
 - packet byte counts, 367
 - protocol byte counts, 367
 - send/receive traffic, 366
 - speed/duplex, 366
 - viewing, 365–366
 - logs, 363
 - application logs, 363
 - audit logs, 361
 - Event Viewer logs, 360
 - reviews, 360
 - security logs, 364
 - syslog, 361–363
 - system logs, 364
 - traffic logs, 360
 - NetFlow, 368
 - ports, Ethernet switches, 307–309
 - SNMP, 356
 - community strings, 357–358
 - Get messages, 357
 - MIB, 356–357
 - OID, 357
 - security, authentication, 359
 - security, authNoPriv, 358
 - security, authPriv, 358
 - security, encryption, 359
 - security, integrity, 359
 - security, levels, 358

- security, models, 358
- security, noAuthNoPriv, 358
- Set messages, 357
- SNMP agent, 356
- SNMP manager, 356
- SNMPv1, 357–358
- SNMPv2c, 357–358, 359
- SNMPv3, 358–360
- Trap messages, 357
- walks, 357
- motion detection, 486
- MOU (Memorandum of Understanding), 387
- MPLS (Multiprotocol Label Switching), 40, 41
 - CE routers, 41
 - CPE, 41
 - elements of (overview), 41
 - ELSR, 41
 - label switching, 40
 - LSR, 41
 - P routers, 41
 - PE routers, 41
 - sample topology, 40
 - shim headers, 40
- MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), 478
- MSS (Managed Security Service), 433
- MSSP (Managed Security Service Providers), 433
- MTBF (Mean Time Between Failures), 394
- MTRJ (Mechanical Transfer Registered Jacks), 90–91
- MTTF (Mean Time To Failure), 394
- MTTR (Mean Time to Repair), 394
- MTU (Maximum Transition Units), 11, 12
- multicast flooding, troubleshooting, 565
- multicast groups, 118
- multicast IP addresses, 118, 152–153
- multifactor authentication (MFA), 428, 478
- multilayer switches, 231–232, 234, 243
- multimeters, 512–513
- multimode delay distortion, 89
- multimode fiber-optic cable, 87–89
- multipathing, 337, 396
- multiplexing

- CWDM, 68, 96
- DWDM, 68, 96
- fiber-optic cable, 95–96
- physical layer (OSI model), 10
 - FDM, 11
 - OFDM, 11
 - StatTDM, 11
 - TDM, 10
- spatial multiplexing, 332
- TDM, 68
- WDM, 96

- multitenancy, cloud computing, 215
- MU-MIMO (Multi-User MIMO), 332
- MX records, DNS, 187
- MySQL, 167, 171

N

- NaaS (Network as a Service), 60
- NAC (Network Access Control), 427, 477
- NAS (Network-Attached Storage), 43, 57
- NAT (Network Address Translation), 145
 - classifying NAT IP addresses, 146–147
 - DNAT, 147
 - names of (overview), 146
 - SNAT, 147
 - topologies, 145–146
- NCP (Network Control Protocol), 22
- NDA (Non-Disclosure Agreements), 385
- NDP (Neighbor Discovery Protocol), 151, 293
- neighbors
 - advertisements, 151
 - soliciting, 151
- NetBEUI (NetBIOS Extended User Interface), 20
- NetBIOS (Network Basic Input/Output System), 20
- netcams (IP cameras), 246
- NetFlow, 368
 - analysis application, 368
 - analyzers, 522
 - flow collectors, 368
 - flow exporters, 368
- netstat command, 535–537
- network addresses
 - calculating, 114

- network devices, 293
- network availability (uptime)
 - case studies, 368, 410–411
 - content caching, 401
 - environmental monitors, 354, 365
 - HA, 394
 - backups, 400
 - best practices, 400–401
 - design considerations, 399–400
 - fault-tolerant network design, 395–396
 - hardware redundancy, 397
 - Layer 3 redundancy, 398–399
 - measuring, 394
 - MTBF, 394
 - MTTF, 394
 - MTTR, 394
 - RPO, 395
 - RTO, 395
 - SLA, 394
 - hardware redundancy, 402–403
 - interface statistics/statuses, 367
 - CRC, 367
 - encapsulation errors, 367
 - giants, 367
 - link-state, 366
 - packet byte counts, 367
 - protocol byte counts, 367
 - send/receive traffic, 366
 - speed/duplex, 366
 - viewing, 365–366
 - load balancing, 401–402
 - logs, 363
 - application logs, 363
 - audit logs, 361
 - Event Viewer logs, 360
 - reviews, 360
 - security logs, 364
 - syslog, 361–363
 - system logs, 364
 - traffic logs, 360
 - NetFlow, 368
 - performance metrics, 354
 - bandwidth, 355
 - baselines, 356
 - CPU usage, 354
 - jitter, 355
 - latency (delay), 355
 - memory, 355
 - temperature, 354
- SNMP, 356
 - community strings, 357–358
 - Get messages, 357
 - MIB, 356–357
 - OID, 357
 - security, authentication, 359
 - security, authNoPriv, 358
 - security, authPriv, 358
 - security, encryption, 359
 - security, integrity, 359
 - security, levels, 358
 - security, models, 358
 - security, noAuthNoPriv, 358
 - Set messages, 357
 - SNMP agent, 356
 - SNMP manager, 356
 - SNMPv1, 357–358, 359
 - SNMPv2c, 357–358, 359
 - SNMPv3, 358–360
 - Trap messages, 357
 - walks, 357
- SOHO network design, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
- network devices, 221–222
 - AP, 234, 243
 - bridges, 223–225, 234, 242
 - broadcast domains, 293
 - BYOD policies, 382

- cameras, 246
- case studies, 248–249
- firewalls, 238, 243
- full-duplex mode, 289
- half-duplex mode, 289
- hubs, 222–223, 234, 242, 243
- HVAC sensors, 246
- ICS, 248
- IDS, 239, 243
 - anomaly-based detection, 242
 - categories, 241–242
 - IPS versus, 239–240
 - network placement, 239–240
 - policy-based detection, 241
 - signature-based detection, 241
- IoT technologies, 246–247
- IPS, 239, 243
 - anomaly-based detection, 242
 - categories, 241–242
 - IDS versus, 239–240
 - network placement, 239–240
 - policy-based detection, 241
 - signature-based detection, 241
- Layer 2 switches, 225–231, 234, 243
- Layer 3 capable switches, 231–232, 234, 243
- load balancers, 235, 243
- media converters, 243
- modems
 - cable modems, 235–236, 243
 - DSL modems, 235, 243
- multilayer switches, 231–232, 234, 243
- network addresses, 293
- physical access control, 245–246
- printers, 245
- proxy servers, 237–238
- routers, 233, 234, 243
- SCADA, 248
- VoIP devices/protocols, 244–245
- VPN
 - concentrators, 236–237, 243
 - headends, 236–237
- WAP, 234
- WLC, 235, 243
- network hardening, 453
 - ACL, 457
 - antenna placement, 458
 - AP, 458
 - best practices, 454–457
 - captive portals, 459
 - case studies, 459
 - common passwords/usernames, 454
 - CoPP, 456
 - credentials (default), changing, 454
 - DAI, 456
 - default VLAN, changing, 457
 - DHCP snooping, 456
 - EAP, 458
 - firewall rules, 457
 - geofencing, 459
 - guest network isolation, 458
 - IoT, 458–459
 - keys/credentials (new), generating, 455
 - MAC filtering, 458
 - NIST Digital Identity Guidelines, 454
 - patches, 454
 - ports
 - security, 456
 - unneeded switch ports, disabling, 455
 - power levels, adjusting, 458
 - PSK rotation, 458
 - RA Guard, 456
 - role-based access, 457
 - secure protocols, 455
 - SNMP, 455
 - STP, 456
 - updating, 454
 - upgrading, firmware, 454–455
 - VLAN
 - private VLAN, 456
 - segmentation, 456
 - wireless client isolation, 458
 - wireless security, 458–459
- network interface layer, TCP/IP stack, 22
- network layer (OSI model), 15, 17
 - circuit switching, 15
 - connection services, 16
 - flow control, 16
 - logical addressing, 15
 - message switching, 16
 - packet reordering, 16

- packet switching/routing, 15
- route discovery/selection, 16
- switching, 15–16
- network platform commands, 543
- network segmentation enforcement, defense-
in-depth security, 427
- network services, 181
 - case studies, 191
 - DHCP, 182
 - DORA acronym, 184
 - dynamic address assignment, 182
 - IP addresses, obtaining from DHCP
servers, 182–183
 - IP helpers/DHCP relays, 183–184
 - leases, 184
 - Obtain a DNS address automatically, 184
 - Obtain an IP address automatically,
184–185
 - relay agents, 183–184
 - reservations, 184
 - scope, 184
 - static address assignment, 182
 - disabling unneeded services, 455
 - DNS
 - A records, 187
 - AAAA records, 187
 - authoritative domain servers, 187
 - CNAME records, 187
 - DDNS, 188
 - DNS TTL, 189
 - EDNS, 188
 - external DNS servers, 187
 - forward lookups, 189
 - FQDN, 185–186, 189
 - global DNS systems, 189
 - global hierarchy, 186–187
 - internal DNS servers, 187
 - IP addressing, 188
 - IPAM, 188
 - iterative lookups, 190
 - MX records, 187
 - NS records, 187
 - PTR records, 188
 - record types (overview), 187–188
 - recursive lookups, 190
 - reverse lookups, 189
 - root DNS servers, 187
 - servers, 182
 - SOA records, 188
 - SRV records, 188
 - TXT records, 188
 - URL, 189
 - zone transfers, 189
 - locating, 129
 - NTP, 190
 - clients, 190
 - configuring, 190
 - ports, 190
 - servers, 190
 - stratum, 190
 - UDP, 190
 - unneeded services, disabling, 455
- network sniffers, 307, 520–521
- networks, 35
 - ACL, troubleshooting, 564
 - architectures, 197
 - case studies, 206
 - collapsed core design, 200
 - deciding on, 205–206
 - SAN, 204–205
 - SDN, 200–202
 - spine and leaf topologies, 202–204
 - three-tiered network architectures,
198–200
 - asymmetrical routing, troubleshooting, 565
 - blocked IP addresses, troubleshooting, 564
 - broadcast storms, troubleshooting, 565
 - BYOD policies, troubleshooting, 566
 - CAN, 39
 - case studies, 69, 566–567
 - characteristics of, 37
 - client/server networks, 42–43
 - collisions, troubleshooting, 565
 - command line tools, 522, 537
 - arp command, 533–535
 - case studies, 543
 - dig command, 531–532
 - ifconfig command, 528–529
 - ip command, 529
 - ipconfig command, 524–528

- ipconfig/all command, 526–527
- ipconfig/release command, 527–528
- netstat command, 535–537
- nmap command, 542
- nslookup [fqdn] command, 529–531
- nslookup command, 529, 531
- ping command, 523–524
- route add command, 541–542
- route command, 538–542
- route delete command, 540–541
- route print command, 538–540
- tcpdump command, 542
- tracert command, 532–533
- configuration/performance baselines, 387
- defined, 36
- defined based on resource location, 42–45
- device configurations, troubleshooting, 562
- DHCP servers, troubleshooting, 564
- faults, 394
- fault-tolerant network design, 395
 - no single point of failure, 396
 - single points of failure, 395–396
- Fibre Channel, 57
- firewalls, troubleshooting, 564
- goodput, 337
- guest network isolation, 458
- hardware, failures, troubleshooting, 566
- HFC networks, 64
- hubs, 11
- hybrid networks, 45, 54
- IDS placement, 239–240
- interface status, troubleshooting, 562–563
- IP addresses (blocked), troubleshooting, 564
- IPS placement, 239–240
- iSCSI, 57
- LAN
 - AP, 234, 243
 - bridges, 223–225
 - sample topology, 37–38
 - WLC, 235, 243
- licensed features, troubleshooting, 566
- loss budgets, troubleshooting, 566
- low optical link budgets, troubleshooting, 566
- MAN, 39
- mGRE, 41
- missing routes, troubleshooting, 566
- MPLS, 40, 41
 - CE routers, 41
 - CPE, 41
 - elements of (overview), 41
 - ELSR, 41
 - label switching, 40
 - LSR, 41
 - P routers, 41
 - PE routers, 41
 - sample topology, 40
 - shim headers, 40
- multicast flooding, troubleshooting, 565
- NaaS, 60
- NAS, 43, 57
- NFS, 43
- NID, 55–55
- NOS, 43
- overlays, 37
- PAN, 39
- peer-to-peer networks, 43–45
- performance
 - baselines, 563
 - troubleshooting, 563, 566
- platform commands, 543
- PON, 69
- private IP networks, 116
- provider links, 60
 - ADSL, 62–63
 - cable modems, 64–65
 - DSL, 62–63
 - leased lines, 65–67
 - satellite provider links, 60–62
 - SDSL, 63
 - VDSL, 64
- purpose of, 36
- reliability, 394
- routing, troubleshooting
 - asymmetrical routing, 565
 - missing routes, 566
- routing loops, troubleshooting, 565
- routing tables, troubleshooting, 562
- SAN, 38, 204
 - FCoE, 205

- Fibre Channel, 204
- IB, 205
- iSCSI, 205
- SD-WAN, 39–40
- segments, 47
- services, troubleshooting
 - blocked services, 564
 - unresponsive services, 565
- smartjacks, 55
- software tools, 520
 - bandwidth speed testers, 520
 - case studies, 543
 - collectors, 522
 - IP scanners, 521, 522
 - iperf, 521–522
 - NetFlow analyzers, 522
 - network sniffers, 520–521
 - packet capturing, 520–521
 - port scanners, 521
 - protocol analyzers, 520–521
 - terminal emulators, 522
 - TFTP servers, 522
 - WiFi analyzers, 520
- SOHO network design, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
- SONET, 67–69
- SSL certificates, troubleshooting, 564
- store-and-forward networks, 16
- subnets, Ethernet switches, 293
- switching loops, troubleshooting, 565
- topologies
 - bus topologies, 46–48
 - demarcation points, 55
 - full-mesh topologies, 52–53
 - hub-and-spoke topologies, 51–52
 - hybrid networks, 54
 - logical topologies, 45–46
 - partial-mesh topologies, 53–54
 - physical topologies, 45–46
 - ring topologies, 46, 48–49
 - service-related entry points, 55
 - star topologies, 45, 50
 - VoIP, 244
- troubleshooting, 562
 - ACL, 564
 - asymmetrical routing, 565
 - blocked IP addresses, 564
 - blocked services, 564
 - blocked TCP/UDP ports, 564
 - broadcast storms, 565
 - BYOD policies, 566
 - case studies, 566–567
 - collisions, 565
 - device configurations, 562
 - DHCP scope exhaustion, 564
 - duplicate IP addresses, 563
 - duplicate MAC addresses, 563
 - expired IP addresses, 564
 - firewalls, 564
 - hardware failures, 566
 - incorrect time, 564
 - interface status, 562–563
 - licensed features, 566
 - loss budgets, 566
 - low optical link budgets, 566
 - missing routes, 566
 - multicast flooding, 565
 - performance, 566
 - performance baselines, 563
 - rogue DHCP servers, 564
 - routing loops, 565
 - routing tables, 562
 - switching loops, 565
 - TCP ports, 564
 - UDP ports, 564
 - unresponsive services, 565
 - untrusted SSL certificates, 564

- VLAN, 563
- types of (overview), 37
- underlays, 37
- virtual networks, 55
 - off-site options, 60
 - on-site options, 60
 - virtual desktops, 58–60
 - virtual firewalls, 58
 - virtual routers, 58
 - virtual servers, 55–57
 - VNC, 476
 - vSwitches, 58–59
- VLAN
 - 802.1Q standard (dot1q), 297
 - ARP, 293
 - assigning, 563
 - default VLAN, changing, 457
 - Ethernet switches, 293–295
 - hopping, 442
 - NDP, 293
 - port tagging, 297
 - private VLAN, 456
 - segmentation, 456
 - troubleshooting, 563
 - trunks, 296–297
 - voice VLAN, 295
 - VTP, 295
- VPN, 215
 - clientless VPN, 468
 - client-to-site VPN, 466
 - concentrators, 236–237, 243
 - DMVPN, mGRE, 41
 - full tunnel configurations, 468
 - headends, 236–237
 - IPsec site-to-site VPN setup/tear down, 472–473
 - L2F, 474
 - L2TP, 474
 - OpenVPN, 474
 - PPTP, 474
 - remote access, 466–474
 - site-to-site VPN, 466–467, 472–473
 - split tunnel configurations, 468
 - SSL, 474
 - SSTP, 474
 - TLS, 474
- WAN
 - MPLS, 40–41
 - sample topology, 38
 - satellite provider links, 60–62
 - SD-WAN, 39–40
 - wireless networks, troubleshooting, 555
- WLAN, 38, 321–322
 - 802.11 wireless standard, 333
 - 802.11a wireless standard, 331, 333
 - 802.11ac (Wi-Fi 5) wireless standard, 332, 333
 - 802.11ax (Wi-Fi 6) wireless standard, 332, 333
 - 802.11b wireless standard, 331, 333
 - 802.11g wireless standard, 331, 333
 - 802.11n (Wi-Fi 4) wireless standard, 332, 333
 - ad hoc WLAN, 322
 - antennas, 324–326
 - associations, 323
 - case studies, 345–346
 - cellular technologies, 333–334
 - channels, 327–329
 - components of, 322
 - concepts, 322
 - CSMA/CA, 329
 - deploying, 334–339
 - frequencies, 327–329
 - hotspots, 322
 - IBSS WLAN, 322
 - transmission methods, 330–331
 - troubleshooting, 550
 - troubleshooting, antennas, 551
 - troubleshooting, AP association time, 552
 - troubleshooting, AP placement, 554
 - troubleshooting, attenuation, 550
 - troubleshooting, captive portals, 554
 - troubleshooting, case studies, 556
 - troubleshooting, channels, 552
 - troubleshooting, client disassociation issues, 554
 - troubleshooting, deployments, 550–551
 - troubleshooting, distance, 550
 - troubleshooting, EIRP/power settings, 551

- troubleshooting, frequencies, 552
 - troubleshooting, interference, 553
 - troubleshooting, latency, 553
 - troubleshooting, misconfiguration of
 - wireless parameters, 553
 - troubleshooting, multiple paths of
 - propagation, 554
 - troubleshooting, RSSI signal strength, 550
 - troubleshooting, signal strength, 553
 - troubleshooting, site surveys, 552
 - troubleshooting, speed (data rates), 550
 - troubleshooting, throughput, 550
 - WAP, 323–324
 - wireless routers, 322–323
 - WLC, 324
 - WPAN, 39
 - new keys/credentials, generating, 455
 - next-hop IP addresses, 260
 - NFC (Near Field Communication), 247, 345
 - NFS (Network File Systems), 43
 - NFV (Network Function Virtualization), 58
 - NIC (Network Interface Cards)
 - bonding, 397
 - data link layer (OSI model), 14
 - MDI, 85
 - redundancy, 397
 - teaming, 397
 - virtual servers, 55
 - vNIC, 56–57
 - NID (Network Interface Devices), 55
 - NIST, Digital Identity Guidelines, 454
 - nmap command, 542
 - NNTP (Network News Transfer Protocol), 174
 - no single point of failure, 396
 - noAuthNoPriv, 358
 - nondesignated ports, STP, 302, 303
 - Non-Disclosure Agreements (NDA), 385
 - nonoverlapping channels, 328, 338–339
 - nonplenum cable, 86
 - nonroot bridges, 301
 - northbound operations, 201–202
 - north-south traffic flows, 201–202
 - NOS (Network Operating Systems), 43
 - NS records, DNS, 187
 - nslookup [fqdn] command, 529–531
 - nslookup command, 529, 531
 - NTP (Network Time Protocol), 168, 171, 174, 190
 - clients, 190
 - configuring, 190
 - ports, 190
 - servers, 190
 - stratum, 190
 - UDP, 190
 - number of subnets, calculating, 133
 - numbering, binary, 106
 - ARIN, 115
 - converting
 - conversion table, 106
 - to decimal numbers, 107
 - decimal numbers to, 107–109
 - practice exercises, 109–112
 - IANA, 116
 - ICANN, 115
 - principles of, 106
 - Nyquist theorem, 66
- ## O
- obstacles (physical), RFI, 337
 - Obtain a DNS address automatically, 184
 - Obtain an IP address automatically, 184–185
 - octets
 - block size, 137
 - IPv4 addresses, 113
 - subnet masks, 131
 - OFDM (Orthogonal Frequency-Division Multiplexing), 11, 330
 - OFDMA (Orthogonal Frequency-Division Multiple Access), 331
 - off-site options, virtual networks, 60
 - OID (Object Identifiers), 357
 - omnidirectional antennas, 325–326, 551
 - onboarding/offboarding procedures, 384
 - on-path attacks, 441
 - on-site options, virtual networks, 60
 - open authentication, WLAN, 341
 - Open Web Application Security Project (OWASP), 424
 - opens, troubleshooting, 508

- OpenVPN, 474
- optical cables (dirty), troubleshooting, 509
- orchestration, defined, 214
- organizational documents/policies, 375–376
 - audit and assessment reports, 387
 - AUP, 379, 382
 - baseline configurations, 387
 - BCP, 377
 - BYOD policies, 382
 - case studies, 387–388
 - change management plans, 376, 386
 - diagram symbols, 386
 - DLP policies, 380–381
 - DRP, 377
 - fair use policies, 382
 - floor plans, 386
 - hardening/security policies, 378–380
 - IDF documentation, 386
 - incident response plans, 376–377
 - international export controls, 385
 - inventory management, 387
 - labeling, 386
 - licensing restrictions, 384
 - logical network diagrams, 386
 - MDF documentation, 386
 - MOU, 387
 - NDA, 385
 - network configuration/performance
 - baselines, 387
 - onboarding/offboarding procedures, 384
 - password policies, 378–379
 - physical network diagrams, 385, 386
 - port location diagrams, 386
 - PUA, 383
 - rack diagrams, 386
 - remote access policies, 381–382
 - safety procedure policies, 383
 - site surveys, 387, 552
 - SLA, 387, 394
 - SOP, 386
 - system life cycles, 377–378
 - wiring diagrams, 386
 - work instructions, 386
- OSI reference model, 3
 - application layer, 21–22
 - application services, 22
 - service advertisements, 22
 - bookshelf analogy, 4–5
 - data link layer, 11, 12
 - DLC, 12
 - LLC, 13–14
 - MAC, 12–13
 - MTU, 11, 12
 - NIC, 14
 - layers of (overview), 6–7
 - network layer, 15, 17
 - circuit switching, 15
 - connection services, 16
 - flow control, 16
 - logical addressing, 15
 - message switching, 16
 - packet reordering, 16
 - packet switching/routing, 15
 - route discovery/selection, 16
 - switching, 15–16
 - PDU, 7
 - physical layer, 7–8
 - AM modulation, 9
 - asynchronous synchronization, 10
 - bandwidth, 10
 - baseband technologies, 10
 - broadband technologies, 10
 - current state modulation, 8
 - FDM, 11
 - FM modulation, 9
 - multiplexing, 10–11
 - OFDM, 11
 - physical topologies, 9
 - state transition modulation, 8–9
 - StatTDM, 11
 - synchronization bits, 9
 - synchronous synchronization, 10
 - TDM, 10
 - presentation layer, 20–21
 - data formatting, 21
 - encryption, 21
 - session layer, 19
 - maintaining sessions, 19
 - NetBIOS, 20
 - setting up sessions, 19

- SIP, 20
 - tearing down sessions, 19
 - transport layer, 17
 - buffering, 18
 - ICMP, 19
 - TCP, 17
 - UDP, 17
 - windowing, 18
 - value of, 6
 - OSPF (Open Shortest Path First), 268, 270
 - OTDR (Optical Time-Domain Reflectometers), 511–512
 - out-of-band management, 479–480
 - overlaps, channels, 555
 - overlays, 37
 - overt channels, information sent over, 446
 - OWASP (Open Web Application Security Project), 424
- P**
- P (Provider) routers, 41
 - PaaS (Platform as a Service), 213
 - packets
 - byte counts, 367
 - capturing, 307–309, 446, 520–521
 - decapsulation, 28
 - drops, 271
 - HSPA+, 333
 - IPv4 format, 23
 - QoS, 270–272
 - best-effort treatment, 273
 - categories, 274
 - $CIR = Bc / Tc$ formula, 276
 - components of, 273–274
 - configuring, 272–273
 - conforming traffic, 276
 - data, 272–273
 - delay (latency), 270, 271, 273
 - DiffServ, 273
 - drops, packets, 271
 - exceeding traffic, 276
 - IntServ, 273
 - jitter, 271
 - mechanisms, 274–276
 - policing traffic, 275–276
 - priority treatment, 273
 - shaping traffic, 275–276
 - soft QoS, 273
 - $Tc = Bc / CIR$ formula, 276
 - video, 272
 - voice, 272
 - reordering, network layer (OSI model), 16
 - sniffing, 446
 - switching/routing, network layer (OSI model), 15
 - PAN (Personal Area Networks), 39
 - parity bits, 14
 - partial-mesh topologies, 53–54
 - passive hubs, 222
 - passwords
 - attacks, 443
 - common passwords, 454
 - NIST Digital Identity Guidelines, 454
 - policies, 378–379
 - PAT (Port Address Translation), 147–148
 - patch bays, 96
 - patch panels, 96
 - patches, 454
 - path-vector routing protocols, 269
 - PBX (Private Branch Exchanges), 245
 - PC (Physical Contact), fiber-optic cable, 90
 - PDU (Power Distribution Units), SOHO network design, 409
 - PDU (Protocol Data Units), 7
 - PE (Provider Edge) routers, 41
 - peer-to-peer networks, 43–45
 - penetration testing, 432
 - performance
 - exercises/simulations, exam preparation, 573
 - metrics, network availability, 354
 - bandwidth, 355
 - baselines, 356
 - CPU usage, 354
 - jitter, 355
 - latency (delay), 355
 - memory, 355
 - temperature, 354
 - networks
 - baselines, 563

- configuration/performance baselines, 387
 - SOHO network design, 409
 - troubleshooting, 563, 566
- permissions, users, 426
- Personal mode
 - WLAN, 341–342
 - WPA2, 345
- PGP (Pretty Good Privacy), 420
- phishing, 445
- phones
 - analog phones, 245
 - cordless phones, RFI, 337
 - IP phones, 244
- physical addressing, MAC, 12
- physical layer (OSI model), 7–8
 - bandwidth, 10
 - baseband technologies, 10
 - broadband technologies, 10
 - modulation
 - AM modulation, 9
 - current state modulation, 8
 - FM modulation, 9
 - state transition modulation, 8–9
- multiplexing, 10
 - FDM, 11
 - OFDM, 11
 - StatTDM, 11
 - TDM, 10
- physical topologies, 9
- synchronization
 - asynchronous synchronization, 10
 - bits, 9
 - synchronous synchronization, 10
- physical network diagrams, 385, 386
- physical obstacles, RFI, 337
- physical security
 - access control panels (controllers), 245
 - access control vestibules (mantraps), 245, 489
 - asset disposal, 489–490
 - asset tracking tags, 486
 - badge readers, 245, 488
 - biometrics, 488
 - cameras, 246, 486
 - case studies, 490
 - detection methods, 486
 - factory resets, 489
 - HVAC sensors, 246
 - key fobs, 488
 - locking cabinets, 245, 488
 - locking racks, 245, 488
 - locks, 245, 488
 - magnetic door switches, 246
 - mantraps, 245, 489
 - motion detection, 486
 - prevention methods, 486–489
 - RTE devices, 246
 - sanitizing devices for disposal, 489
 - smart cards, 488
 - smart lockers, 488
 - tamper detection, 486
 - wipe configurations, 489
- physical topologies
 - logical topologies versus, 45–46
 - physical layer (OSI model), 9
- piggybacking, 445
- pin mappings, crossover cable, 85
- ping command, 523–524
 - ping of death, 448
 - sweeps, 446
- pinouts, troubleshooting, 508
- pins, troubleshooting, 508
- plans/policies, 376
 - action plans (troubleshooting), 500
 - audit and assessment reports, 387
 - AUP, 379, 382
 - back-out plans, 500
 - baseline configurations, 387
 - BCP, 377
 - BYOD policies, 382
 - case studies, 387–388
 - change management plans, 376, 386
 - diagram symbols, 386
 - DLP policies, 380–381
 - DRP, 377
 - fair use policies, 382
 - final review/study plans
 - exam preparation, 574–575
 - flash card mode, 575
 - practice exam mode, 574

- study mode, 574
- floor plans, 386
- hardening/security policies, 378–380
- IDF documentation, 386
- incident response plans, 376–377
- international export controls, 385
- inventory management, 387
- labeling, 386
- licensing restrictions, 384
- logical network diagrams, 386
- MDF documentation, 386
- MOU, 387
- NDA, 385
- network configuration/performance
 - baselines, 387
- onboarding/offboarding procedures, 384
- password policies, 378–379
- physical network diagrams, 385, 386
- port location diagrams, 386
- PUA, 383
- rack diagrams, 386
- remote access policies, 381–382
- safety procedure policies, 383
- site surveys, 387, 552
- SLA, 387, 394
- SOP, 386
- system life cycles, 377–378
- wiring diagrams, 386
- work instructions, 386
- platform commands, network, 543
- plenum cable, 86, 506–507
- PoE (Power over Ethernet), 306–307, 507
- PoE+ (enhanced PoE), 307
- poison reverses, 267
- poisoning DNS, 442
- polarity, antennas, 326
- polarization, antennas, 551
- policing traffic, 275–276
- policy-based detection, IDS/IPS, 241
- PON (Passive Optical Networks), 69
- POP3 (Post Office Protocol Version 3), 168, 171, 174
- POP3 over SSL, 168, 171
- port numbers, IP addresses, TCP/IP stack, 26–27
- port scanners, 521
- portals (captive), 459, 478, 554
- ports
 - access ports, Ethernet, 295
 - aggregation, 407
 - bad ports, troubleshooting, 508
 - DHCP assignments, 166, 170
 - ephemeral ports, 27
 - FTP bounce, 447
 - H.323 assignments, 166, 170
 - HTTP assignments, 166, 170
 - HTTPS assignments, 167, 170
 - IMAP assignments, 167, 170
 - IMAP over SSL assignments, 167, 170
 - LDAP assignments, 167, 170
 - LDAPS assignments, 167, 171
 - location diagrams, 386
 - MDI, 85
 - MDIX, 85
 - MGCP assignments, 167, 171
 - mirroring, Ethernet switches, 307–309
 - monitoring, Ethernet switches, 307–309
 - MySQL assignments, 167, 171
 - NTP, 168, 171, 190
 - numbers, IP addresses, TCP/IP stack, 26–27
 - POP3 assignments, 168, 171
 - POP3 over SSL assignments, 168, 171
 - RDP, 168, 171
 - scanning attacks, 446
 - security, 456
 - SFTP assignments, 168, 171
 - SIP assignments, 168, 171
 - SMB assignments, 168, 171
 - SMTP assignments, 169, 171
 - SMTP TLS assignments, 169, 171
 - SNMP assignments, 169, 171
 - SQL Server assignments, 169, 171
 - SQLnet assignments, 169, 171
 - SSH assignments, 169, 171
 - STP
 - costs, 302–303
 - designated ports, 302
 - identifying roles, 302
 - long STP, 303

- nondesigned ports, 302, 303
 - root ports, 302
- Syslog assignments, 169, 172
- tagging, 297
- TCP ports, blocked ports, troubleshooting, 564
- Telnet assignments, 170, 172
- TFTP assignments, 170, 172
- UDP ports, troubleshooting, 564
- unneded switch ports, disabling, 455
- well-known ports, 27
- postmortem reports, 501
- posture assessments, 432
- power levels, adjusting, 458
- power supplies, 400
- PPP (Point-to-Point Protocol), 65, 476
- PPPoE (Point-to-Point Protocol over Ethernet), 476
- PPTP (Point-to-Point Tunneling Protocol), 474
- practice exam mode, final review/study plan, 574
- prefix (slash) notation, IPv4 addresses, 114
- preparing for exams, 577
 - end-of-chapter review tools, 573
 - exam taking strategies, 576–577
 - final review/study plan, 574–575
 - memory tables, 572–573
 - simulations/performance-based exercises, 573
 - tools, 571–572
 - video training, 572
- presentation layer (OSI model), 20–21
 - data formatting, 21
 - encryption, 21
- Pretty Good Privacy (PGP), 420
- prevention methods, 487–488
 - access control vestibules (mantraps), 489
 - badge readers, 488
 - biometrics, 488
 - employee training, 486–487
 - key fobs, 488
 - locking cabinets, 488
 - locking racks, 488
 - locks, 488
 - mantraps, 489
 - smart cards, 488
 - smart lockers, 488
- preventive measures, implementing, 500
- printers, 245
- priority treatment
 - QoS, 273
 - traffic, 273
- private clouds, 212
- private IP addresses, 145
- private IP networks, 116
- private VLAN, 456
- privilege, least, 425
- Privileged User Agreements (PUA), 383
- probable cause, theories of
 - establishing, 499
 - testing, 499
- problems
 - diagnosing, 497
 - identifying, 499
- process assessments, 432–433
- programmable infrastructures. *See* IaC
- propagation paths, troubleshooting, 554
- protocol analyzers, 520–521
- protocols
 - ARP
 - DAI, 456
 - VLAN, 293
 - BGP, 269, 270
 - BOOTP, 182
 - byte counts, 367
 - CAPWAP, 324
 - CARP, 313, 398
 - CHAP, 477
 - DHCP, 166, 170, 175, 182–184, 442
 - snooping, 456
 - DNS, 166, 170, 175, 185–190
 - dynamic routing protocols, 261–262
 - EAP, 343, 431, 458, 478
 - ECMP, 396
 - EGP, 263, 264–265
 - EIGRP, 268–269, 270, 396
 - FHRP, 398
 - FTP, 166, 170, 174, 447
 - GLBP, 313, 399

- H.323, 166, 170
- HSRP, 312–313, 398
- HTTP, 166, 170, 174
- HTTPS, 167, 170, 174
- ICMP, attacks, 448
- IGMP, 175
- IGP, 263, 264–265
- IMAP, 167, 170
- IMAP over SSL, 167, 170
- IMAP4, 174
- IP, 173
- IP protocols
 - GRE, 173
 - ICMP, 173, 174
 - IPsec, 173
 - TCP, 172, 174
 - UDP, 172, 174
- ISAKMP, 469–470
- IS-IS, 268
- Kerberos, 477
- L2F, 474
- L2TP, 474
- LACP, 305, 399
- LDAP, 167, 170, 175, 429, 478
- LDAPS, 167, 171
- LWAPP, 324
- MGCP, 167, 171
- MS-CHAP, 478
- MySQL, 167, 171
- NDP, VLAN, 293
- NNTP, 174
- NTP, 168, 171, 174, 190
- OpenVPN, 474
- OSPF, 268, 270
- POP3, 168, 171, 174
- POP3 over SSL, 168, 171
- PPP, 476
- PPPoE, 476
- PPTP, 474
- RDP, 168, 171, 475
- RIP, 268, 270
- routing protocols
 - BGP, 269, 270
 - characteristics of, 263
 - distance-vector routing protocols, 265–267
 - EIGRP, 268–269, 270
 - IS-IS, 268
 - link-state routing protocols, 268
 - metrics, 263, 264
 - OSPF, 268, 270
 - path-vector routing protocols, 269
 - RIP, 268, 270
- RSTP, 298
- RTP, 245
- SCP, 174
- secure protocols, network hardening, 455
- SFTP, 168, 171, 174
- Shortest Path Bridging, 299
- SIP, 168, 171, 175, 245
- SMB, 168, 171
- SMTP, 169, 171, 174
- SMTP TLS, 169, 171
- SNMP, 169, 171, 175, 356
 - community strings, 357–358
 - Get messages, 357
 - MIB, 356–357
 - network hardening, 455
 - OID, 357
 - secure SNMP, 455
 - security, authentication, 359
 - security, authNoPriv, 358
 - security, authPriv, 358
 - security, encryption, 359
 - security, integrity, 359
 - security, levels, 358
 - security, models, 358
 - security, noAuthNoPriv, 358
 - Set messages, 357
 - SNMP agent, 356
 - SNMP manager, 356
 - SNMPv1, 357–358, 359
 - SNMPv2c, 357–358, 359
 - SNMPv3, 358–360
 - Trap messages, 357
 - walks, 357
- SQL Server, 169, 171
- SQLnet, 169, 171
- SSH, 169, 171, 174, 476
- SSL, 474
- SSTP, 474
- STP, 298–299, 456

- Syslog, 169, 172
- TCP flooding, 448
- TCP/IP protocol suite (summary), 173–175
- Telnet, 170, 172, 174
- TFTP, 170, 172, 174
- TKIP, 344
- TLS, 175, 474
- UDP, NTP, 190
- VoIP, 244–245
- VRRP, 313, 398
- VTP, trunks, 295
- provider links, 60
 - cable modems, 64–65
 - DSL, 62
 - ADSL, 62–63
 - VDSL, 64
 - leased lines, 65
 - DSo, 65
 - E1 circuits, 66–67
 - E3 circuits, 67
 - HDLC, 66
 - PPP, 65
 - T1 circuits, 66
 - T3 circuits, 67
 - metro-optical, 67
 - satellite provider links
 - delay, 61
 - sample WAN topology, 60–61
 - weather sensitivity, 61–62
 - SDSL, 63
 - SONET, 67–69
- proxies, reverse, 238
- proxy servers, 237–238
- PSK (Preshared Keys)
 - rotating, 458
 - WLAN, 341–342
- PTR records, DNS, 188
- PUA (Privileged User Agreements), 383
- public clouds, 212
- punchdown blocks, 96
- punchdown tools, 509

Q

- Q-in-Q tunneling, 442
- QoS (Quality of Service), 270–272

- best-effort treatment, 273
- categories, 274
- $CIR = Bc / Tc$ formula, 276
- components of, 273–274
- configuring, 272–273
- conforming traffic, 276
- data, 272–273
- delay (latency), 270, 271, 273
- DiffServ, 273
- drops, packets, 271
- Ethernet switches, 314
- exceeding traffic, 276
- IntServ, 273
- jitter, 271
 - mechanisms, 274–276
 - policing traffic, 275–276
 - priority treatment, Low Delay, 273
 - shaping traffic, 275–276
 - soft QoS, 273
 - $Tc = Bc / CIR$ formula, 276
- video, 272
- voice, 272
- QSFP (Quad SFP), 95
- QSFP+ (Enhanced QSFP), 95
- queues. *See* buffering
- Quick mode, IPsec with IKE, 469

R

- RA (Router Advertisement) Guard, 456
- rack diagrams, 386
- racks, locking, 245, 488
- RADIUS (Remote Authentication Dial-In User Service), 342, 429, 477
- ransomware, 443
- RARP (Reverse Address Resolution Protocol), 128
- RBAC (Role-Based Access Control), 425–426
- RC4 encryption, 343–344
- RDBMS (Relational Database Management Systems), MySQL, 167, 171
- RDC (Remote Desktop Connections), 475
- RDP (Remote Desktop Protocol), 168, 171, 475
- readers, badge, 245, 488
- real transfer time, 18

- real-world case studies
 - architectures, network, 206
 - attacks, 449
 - availability, network, 368
 - cabling, 99, 514
 - cloud computing, 217
 - command line tools, 543
 - corporate architectures, 206
 - datacenter architectures, 206
 - disaster recovery, 410–411
 - documentation, 387–388
 - Ethernet switches, 314–315
 - IP addressing, 154
 - monitoring, 368
 - network availability, 368, 410–411
 - network devices, 248–249
 - network hardening, 459
 - network platform commands, 543
 - network services, 191
 - network topologies, 69
 - network troubleshooting, 566–567
 - organizational documents/policies, 387–388
 - physical security, 490
 - plans/policies, 387–388
 - reference models, 27–28
 - remote access, 480
 - routing, 276–277
 - security, 434–459
 - software tools, 543
 - SOHO network design, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
 - troubleshooting, 501, 556
 - wireless standards, 345–346
 - WLAN, 345–346, 556
- receive (Rx) reads, troubleshooting, 509
- receive/send traffic statistics/statuses, 366
- reconnaissance attacks, 446
- record types (overview), DNS, 187–188
- recovery
 - cold sites, 402
 - warm sites, 402
- Recovery Point Objective (RPO), 395
- Recovery Time Objective (RTO), 395
- recursive lookups, 190
- redirects, 151
- redistributing routes, 270
- redundancy
 - CARP, 313, 398
 - CRC, 14, 367
 - FHRP, 398
 - first-hop redundancy, Ethernet switches, 312–313
 - GLBP, 399
 - hardware, 397, 402–403
 - HSRP, 398
 - LACP, 399
 - Layer 3 redundancy, 398–399
 - NIC, 397
 - routing, 262
 - VRRP, 313, 398
- reference models
 - case studies, 27–28
 - DoD model. *See* TCP/IP stack
 - NCP, 22
 - OSI reference model, 3
 - application layer, 21–22
 - bookshelf analogy, 4–5
 - data link layer, 11–14
 - layers of (overview), 6–7
 - network layer, 15–17
 - PDU, 7
 - physical layer, 7–11
 - presentation layer, 20–21
 - session layer, 19–20
 - transport layer, 17–19
 - value of, 6
 - purpose of, 4–6

- TCP/IP stack, 22, 25
 - application layer, 25
 - application protocols, 26–27
 - Internet layer, 23
 - IP addresses, 26–27
 - layers of (overview), 22–25
 - network interface layer, 22
 - port numbers, 26–27
 - transport layer, 24–25
- reflective DoS attacks, 440
- reflectometers, 511–512
- refractive index, fiber-optic cable, 87
- relay agents, DHCP, 183–184
- reliability, networks, 394
- reliable transport, TCP, 172
- remote access, 465, 474–475
 - 802.1X user authentication, 477
 - AAA, 477
 - authentication, 478–479
 - authorization, 478–479
 - captive portals, 478
 - case studies, 480
 - CHAP, 477
 - EAP, 478
 - ICA, 476
 - in-band management, 479–480
 - IPsec
 - AH, 470–471
 - ESP, 470–471
 - IKE, 468–470, 472–473
 - Kerberos, 477
 - LDAP, 478
 - local authentication, 478
 - MFA, 478
 - MS-CHAP, 478
 - NAC, 477
 - out-of-band management, 479–480
 - PPP, 476
 - PPPoE, 476
 - RADIUS, 477
 - RDC, 475
 - RDP, 475
 - remote desktop gateways, 475
 - RRAS, 475
 - SSH, 476
 - SSO, 478
 - TACACS+, 477
 - TFA, 478
 - virtual desktops, 476
 - VNC, 476
 - VPN, 466
 - clientless VPN, 468
 - client-to-site VPN, 466
 - IPsec site-to-site VPN setup/tear down, 472–473
 - site-to-site VPN, 466–467
- remote access policies, 381–382
- Remote Authentication Dial-In User Service (RADIUS), 342, 429, 477
- remote desktops
 - gateways, 475
 - RDC, 475
 - RDP, 475
- reordering packets, network layer (OSI model), 16
- repeaters (hubs), 222–223, 234, 242, 243
- reports
 - audit and assessment reports, 387
 - postmortem reports, 501
- requests, ARP, 256–257
- reservations, DHCP, 184
- resets, factory, 489
- responders, 469
- restrictions, licensing, 384
- reverse lookups, 189
- reverse proxies, 238
- review tools (exam preparation), end-of-chapter, 573
- reviews, logs, 360
- RF attenuation, 550
- RFC 1918, 145
- RFI (Radio Frequency Interference), 80, 336–337
- RFID (Radio Frequency Identification), 247
- RG-6 coaxial cables, 81
- RG-58 coaxial cables, 81
- RG-59 coaxial cables, 80
- ring topologies, 46, 48–49
- RIP (Routing Information Protocol), 268, 270
- riser rated cabling, 507

- risk management, 431
 - business risk assessments, 432–433
 - penetration testing, 432
 - posture assessments, 432
 - process assessments, 432–433
 - threat assessments, 431
 - vendor assessments, 431
 - vulnerability assessments, 432
- RJ11 connectors, 85–86
- RJ45 connectors, 9, 85–86
- roaming, 338
- rogue AP, 340, 443
- rogue DHCP servers, 442, 564
- role-based access, 457
- Role-Based Access Control (RBAC), 425–426
- rollover cable, 507
- root bridges, 301
- root DNS servers, 187
- root ports, STP, 302
- rotating PSK, 458
- route add command, 541–542
- route aggregation. *See* CIDR
- route command, 538–542
- route delete command, 540–541
- route discovery/selection, network layer (OSI model), 16
- route print command, 538–540
- routers, 233, 234, 243
 - active routers, 312
 - advertisements, 151
 - CE routers, 41
 - ELSR, 41
 - HSRP, 398
 - LSR, 41
 - P routers, 41
 - PE routers, 41
 - RA Guard, 456
 - redirects, 151
 - soliciting, 151
 - standby routers, 312
 - subinterfaces, 120
 - virtual routers, 58
 - VRRP, 313
 - wireless routers, 322–323
- routing, 255
 - AD, 263
 - advertising methods, 264–268
 - ARP requests, 256–257
 - asymmetrical routing, troubleshooting, 565
 - bandwidth management. *See* QoS
 - basic routing process, 256–259
 - believability of routes, 263
 - BGP, 269, 270
 - case studies, 276–277
 - CIDR, 144
 - default static routes, 260
 - Dijkstra’s shortest path first algorithm, 268
 - directly connected routes, 259
 - distance-vector routing protocols, 265–267.
 - See also* EIGRP
 - dynamic routing, 259, 261–262
 - EGP, 263, 264–265
 - EIGRP, 268–269, 270
 - global routing tables, 427
 - hold-down timers, 265
 - hop counts, 262, 266
 - hybrid routing protocols. *See* EIGRP
 - IGP, 263, 264–265
 - IP routing tables, 259
 - IS-IS, 268
 - Layer 3 to Layer 2 mapping, 259
 - link-state routing protocols, 268
 - loops, 266–267
 - LSA, 268
 - missing routes, troubleshooting, 566
 - multipathing, 396
 - next-hop IP addresses, 260
 - OSPF, 268, 270
 - path-vector routing protocols, 269
 - poison reverses, 267
 - process of, 256–259
 - protocols
 - BGP, 269, 270
 - characteristics of, 263
 - distance-vector routing protocols, 265–267
 - EIGRP, 268–269, 270
 - IS-IS, 268
 - link-state routing protocols, 268
 - metrics, 263, 264

- OSPF, 268, 270
 - path-vector routing protocols, 269
 - RIP, 268, 270
 - QoS, 270–272
 - best-effort treatment, 273
 - categories, 274
 - $CIR = Bc / Tc$ formula, 276
 - components of, 273–274
 - configuring, 272–273
 - conforming traffic, 276
 - data, 272–273
 - delay (latency), 270, 271, 273
 - DiffServ, 273
 - drops, packets, 271
 - exceeding traffic, 276
 - IntServ, 273
 - jitter, 271
 - mechanisms, 274–276
 - policing traffic, 275–276
 - priority treatment, 273
 - shaping traffic, 275–276
 - soft QoS, 273
 - $Tc = Bc / CIR$ formula, 276
 - video, 272
 - voice, 272
 - redistributing routes, 270
 - redundancy, 262
 - RIP, 268, 270
 - RRAS, 475
 - split horizons, 267
 - static routes, 260
 - steps of, 256–259
 - topologies, 256
 - TTL, 257–258
 - routing loops, 266–267, 565
 - routing tables, troubleshooting, 562
 - routing/packet switching, network layer (OSI model), 15
 - RPO (Recovery Point Objective), 395
 - RRAS (Routing and Remote Access Server), 475
 - RS-232, DB-9 connectors, 85–86
 - RSSI (Received Signal Strength Indication), WLAN, troubleshooting, 550
 - RSTP (Rapid Spanning Tree Protocol), 298
 - RTE (Request-To-Exit) devices, 246
 - RTO (Recovery Time Objective), 395
 - RTP (Real-time Transport Protocol), 245
 - RTT (Round-Trip Time), 18
 - rules, firewalls, 457
- ## S
- SaaS (Software as a Service), 213
 - safety procedure policies, 383
 - salami attacks, 447
 - SAN (Storage Area Networks), 38, 204
 - FCoE, 205
 - Fibre Channel, 204
 - IB, 205
 - iSCSI, 205
 - sanitizing devices for disposal, 489
 - satellite provider links
 - delay, 61
 - sample WAN topology, 60–61
 - weather sensitivity, 61–62
 - SC (Subscriber Connectors), 90–91
 - SCADA (Supervisory Control and Data Acquisition), 248
 - scalability, cloud computing, 216
 - scanners
 - IP scanners, 521, 522
 - port scanners, 521
 - scanning attacks, ports, 446
 - scope
 - DHCP servers, 184
 - exhaustion, troubleshooting, 564
 - SCP (Secure Copy Protocol), 174
 - screened subnets, defense-in-depth security, 427
 - SDH (Synchronous Digital Hierarchy), 68
 - SDN (Software-Defined Networking), 200–201, 202
 - application layer, 201
 - control layer, 201–202
 - infrastructure layer, 202
 - management layer, 202
 - SDSL (Symmetric SDL), 63
 - SD-WAN (Software-Defined WAN), 39–40
 - SECaaS (Security as a Service), 433
 - security

- access control hardware
 - badge readers, 488
 - biometrics, 488
- attacks
 - ARP spoofing, 442
 - botnets, 441
 - brute-force password attacks, 443
 - buffer overflows, 448
 - case studies, 449
 - command and control software, 441
 - confidentiality attacks, 446
 - data diddling, 447
 - DDoS attacks, 441
 - deauthentication attacks, 444
 - dictionary password attacks, 443
 - DNS poisoning, 442
 - DoS attacks, 440–441
 - dumpster diving, 446
 - electrical disturbances, 448
 - EMI interception, 446
 - environmental-based attacks, 445
 - evil twins (rogue AP), 443
 - FTP bounce, 447
 - human-based attacks, 445
 - ICMP attacks, 448
 - information sent over covert channels, 447
 - information sent over overt channels, 446
 - IP spoofing, 444
 - logic bombs, 448
 - MAC spoofing, 444
 - malware, 444–445
 - Man-in-the-Middle (MitM) attacks.
 - See* on-path attacks
 - packet capturing, 446
 - packet sniffing, 446
 - password attacks, 443
 - on-path attacks, 441
 - phishing, 445
 - piggybacking, 445
 - ping of death, 448
 - ping sweeps, 446
 - port scanning, 446
 - ransomware, 443
 - reconnaissance attacks, 446
 - rogue AP, 443
 - salami attacks, 447
 - scanning attacks, 446
 - session hijacking, 447
 - shoulder surfing, 445
 - Smurf attacks, 448
 - SYN flooding, 448
 - tailgating, 445
 - TCP flooding, 448
 - technology-based attacks, 440–445
 - trust relationship exploitation, 448
 - VLAN hopping, 442
 - wiretapping, 446
 - zero-day attacks, 424
 - zombies, 441
- authentication, 428
 - 802.1X user authentication, 430
 - EAP, 431
 - Kerberos, 429–430
 - LDAP, 429
 - local authentication, 430
 - MFA, 428
 - RADIUS, 429
 - SSO, 429
 - TACACS+, 429
- case studies, 434–459
- CIA, 418
 - availability, 423
 - confidentiality, 418–422
 - integrity, 422–423
- cloud computing, 216
- defense-in-depth security, 426
 - honeynets, 428
 - honeypots, 428
 - NAC, 427
 - network segmentation enforcement, 427
 - screened subnets, 427
 - separation of duties, 427
- encryption, 419
 - 3DES, 419
 - AES, 419
 - asymmetric encryption, 420–422
 - DES, 419
 - GPG, 420

- PGP, 420
 - symmetric encryption, 419–420, 422
- ESP, 470–471
- exploits, 424
- firewalls, 238, 243
 - explicit deny, 457
 - implicit deny, 457
 - rules, 457
- geofencing, 459
- hardening networks, 453
 - ACL, 457
 - antenna placement, 458
 - AP, 458
 - best practices, 454–457
 - captive portals, 459
 - case studies, 459
 - common passwords/usernames, 454
 - CoPP, 456
 - credentials (default), changing, 454
 - DAI, 456
 - default VLAN, changing, 457
 - DHCP snooping, 456
 - EAP, 458
 - firewall rules, 457
 - geofencing, 459
 - guest network isolation, 458
 - IoT, 458–459
 - keys/credentials (new), generating, 455
 - MAC filtering, 458
 - NIST Digital Identity Guidelines, 454
 - patches, 454
 - port security, 456
 - power levels, adjusting, 458
 - private VLAN, 456
 - PSK rotation, 458
 - RA Guard, 456
 - role-based access, 457
 - secure protocols, 455
 - SNMP, 455
 - STP, 456
 - unnneeded switch ports, disabling, 455
 - updating, 454
 - upgrading firmware, 454–455
 - VLAN segmentation, 456
 - wireless client isolation, 458
 - wireless security, 458–459
- HVAC sensors, 246
- IDS, 239, 243
 - anomaly-based detection, 242
 - categories, 241–242
 - IPS versus, 239–240
 - network placement, 239–240
 - policy-based detection, 241
 - signature-based detection, 241
- IoT, 458–459
- IPS, 239, 243
 - anomaly-based detection, 242
 - categories, 241–242
 - IDS versus, 239–240
 - network placement, 239–240
 - policy-based detection, 241
 - signature-based detection, 241
- IPsec
 - AH, 470–471
 - IKE, 468–470, 472–473
- least privilege, 425
- log management, 433
- logs, 364
- MSS, 433
- MSSP, 433
- passwords
 - common passwords, 454
 - NIST Digital Identity Guidelines, 454
- physical security
 - access control panels (controllers), 245
 - access control vestibules (mantraps), 245, 489
 - asset disposal, 489–490
 - asset tracking tags, 486
 - badge readers, 245, 488
 - biometrics, 488
 - cameras, 246, 486
 - case studies, 490
 - detection methods, 486
 - factory resets, 489
 - key fobs, 488
 - locking cabinets, 245, 488
 - locking racks, 245, 488
 - locks, 245, 488
 - magnetic door switches, 246

- mantraps, 245, 489
- motion detection, 486
- prevention methods, 486–489
- RTE devices, 246
- sanitizing devices for disposal, 489
- smart cards, 488
- smart lockers, 488
- tamper detection, 486
- wipe configurations, 489
- policies, 378–380
- ports, 456
- PSK, 458
- RBAC, 425–426
- risk management, 431
 - business risk assessments, 432–433
 - penetration testing, 432
 - posture assessments, 432
 - process assessments, 432–433
 - threat assessments, 431
 - vendor assessments, 431
 - vulnerability assessments, 432
- SECaaS, 433
- SEM, 433
- SIEM, 433
- SIM, 433
- SNMP
 - authentication, 359
 - authNoPriv, 358
 - authPriv, 358
 - encryption, 359
 - integrity, 359
 - noAuthNoPriv, 358
 - security level, 358
 - security model, 358
- syslog, 361–362
- threats, 423
- user permissions, 426
- vulnerabilities, 423–424
- wireless security, 458–459
- wireless security system devices, RFI, 337
- WLAN, 339
 - 802.1X user authentication, 342–343
 - EAP, 343
 - ESSID, 341
 - geofencing, 345
 - issues, 339–341
 - MAC address filtering, 341
 - open authentication, 341
 - Personal mode, 341–342
 - PSK, 341–342
 - RADIUS, 342
 - RC4 encryption, 343–344
 - rogue AP, 340
 - SSID, 340–341
 - standards (overview), 343
 - war chalking, 339–340
 - war dialing, 339
 - war driving, 339
 - war flying, 340
 - WEP, 340, 343–344
 - WPA, 340, 344
 - WPA2, 345
 - WPA3, 342
 - Zero Trust, 426
- Security Information and Event Management (SIEM), 433
- segmentation, 27
 - network segments, 47
 - VLAN, 456
- SEM (Security Event Manager), 433
- send/receive traffic statistics/statuses, 366
- sensors, HVAC, 246
- separation of duties, defense-in-depth security, 427
- servers
 - authentication servers, 310, 430, 477
 - authoritative domain servers, 187
 - DHCP servers
 - IP addresses, obtaining from DHCP servers, 182–183
 - rogue DHCP servers, 442
 - rogue DHCP servers, troubleshooting, 564
 - scope, 184
 - DiffServ, 273
 - DNS servers, 185–186
 - A records, 187
 - AAAA records, 187
 - authoritative domain servers, 187
 - CNAME records, 187

- DDNS, 188
- EDNS, 188
- external DNS servers, 187
- forward lookups, 189
- internal DNS servers, 187
- IP addressing, 188
- IPAM, 188
- iterative lookups, 190
- MX records, 187
- NS records, 187
- PTR records, 188
- record types (overview), 187–188
- recursive lookups, 190
- reverse lookups, 189
- root DNS servers, 187
- SOA records, 188
- SRV records, 188
- TXT records, 188
- external DNS servers, 187
- IIS, 56
- internal DNS servers, 187
- NTP, 190
- proxy servers, 237–238
- root DNS servers, 187
- RRAS, 475
- syslog, 361, 363
- TFTP servers, 522
- virtual servers, 55–57
- service advertisements, application layer (OSI model), 22
- Service-Level Agreements (SLA), 387, 394
- service-related entry points, 55
- services
 - blocked services, troubleshooting, 564
 - cloud computing, 213
 - DaaS, 213
 - IaaS, 213
 - IntServ, 273
 - network services, 181
 - case studies, 191
 - DHCP, 182–184
 - disabling unneeded services, 455
 - DNS, 185–190
 - NTP, 190
 - unneeded services, disabling, 455
 - PaaS, 213
 - SaaS, 213
 - troubleshooting, unresponsive services, 565
 - unresponsive services, troubleshooting, 565
 - XaaS, 213
 - session hijacking, 447
 - session keys, 421
 - session layer (OSI model), 19
 - maintaining sessions, 19
 - NetBIOS, 20
 - setting up sessions, 19
 - SIP, 20
 - tearing down sessions, 19
 - Set messages, 357
 - SF (Super Frame), 66
 - SFP (Small Form-Factor Pluggable), 95, 291
 - SFP+ (enhanced SFP), 95
 - SFTP (Secure FTP), 168, 171, 174
 - SHA-1 (Secure Hashing Algorithm-1), 422
 - shaping traffic, 275–276
 - shim headers, 40
 - Shortest Path Bridging, 299
 - shorthand notation, IPv6 addresses, 150
 - shorts, troubleshooting, 508
 - shoulder surfing, 445
 - show config command, 543
 - show interface command, 543
 - show route command, 543
 - SIEM (Security Information and Event Management), 433
 - signal distance, cabling, 506
 - signal loss, 550
 - signal strength
 - RFI, 337
 - troubleshooting, 553
 - signature-based detection, IDS/IPS, 241
 - signed certificates, 421
 - SIM (Security Information Management), 433
 - simplified troubleshooting flow, 497
 - simulations/performance-based exercises,
 - exam preparation, 573
 - single points of failure, fault-tolerant network design, 395–396
 - Single Sign-On (SSO), 429

- SIP (Session Initiation Protocol), 20, 168, 171, 175, 245
- site surveys, 387, 552
- site-to-site VPN
 - IPsec site-to-site VPN setup/tear down, 472–473
 - remote access, 466–467
- SLA (Service-Level Agreements), 387, 394
- SLAAC (Stateless Address Autoconfiguration), 151
- slash (prefix) notation, IPv4 addresses, 114
- smart cards, 488
- smart hubs, 222
- smart lockers, 488
- smartjacks, 55
- SMB (Server Message Block), 168, 171
- SMF (Single-Mode Fiber) cable, 89, 94
- SMTP (Simple Mail Transfer Protocol), 169, 171, 174
- SMTP TLS, 169, 171
- Smurf attacks, 448
- snapshots, 400
- SNAT (Static NAT), 147
- sniffing, packets, 446
- snips/cutters, 513
- SNMP (Simple Network Management Protocol), 169, 171, 175, 356
 - community strings, 357–358
 - Get messages, 357
 - MIB, 356–357
 - network hardening, 455
 - OID, 357
 - secure SNMP, 455
 - security
 - authentication, 359
 - authNoPriv, 358
 - authPriv, 358
 - encryption, 359
 - integrity, 359
 - levels, 358
 - models, 358
 - noAuthNoPriv, 358
 - Set messages, 357
 - SNMP agent, 356
 - SNMP manager, 356
 - SNMPv1, 357–358, 359
 - SNMPv2c, 357–358, 359
 - SNMPv3, 358–360
 - Trap messages, 357
 - walks, 357
- SOA records, DNS, 188
- soft QoS, 273
- software
 - command and control software, 441
 - SDN, 200–201, 202
 - application layer, 201
 - control layer, 201–202
 - infrastructure layer, 202
 - management layer, 202
- software tools, 520
 - bandwidth speed testers, 520
 - case studies, 543
 - collectors, 522
 - IP scanners, 521, 522
 - iperf, 521–522
 - NetFlow analyzers, 522
 - network sniffers, 520–521
 - packet capturing, 520–521
 - port scanners, 521
 - protocol analyzers, 520–521
 - terminal emulators, 522
 - TFTP servers, 522
 - WiFi analyzers, 520
- SOHO network design, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
- soliciting
 - neighbors, 151

- routers, 151
 - solutions (troubleshooting), implementing, 500
- SONET (Synchronous Optical Networks), 67–69
- SOP (Standard Operating Procedures), 386
- southbound operations, 201–202
- spatial multiplexing, 332
- specifications, cabling, 506
- spectrum analyzers, 513
- speed (data rates)
 - bandwidth speed testers, 520
 - cabling, 506
 - troubleshooting, 509
 - WLAN deployments, troubleshooting, 550
- speed/duplex statistics/statuses, 366
- spine and leaf topologies, 202–204
- splicers, fusion, 513
- split horizons, 267
- split tunnel VPN configurations, 468
- spoke sites, 51
- spoofing
 - ARP, 442
 - IP, 444
 - MAC, 444
- spread spectrum transmissions, 330
 - FHSS, 330
 - OFDM, 330
 - OFDMA, 331
- SQL Server, 169, 171
- SQLnet, 169, 171
- SRV records, DNS, 188
- SSH (Secure Shell), 169, 171, 174, 475, 476
- SSID (Service Set Identifiers), 340–341
 - disabling broadcasts, 341
 - PSK, 341–342
- SSL (Secure Socket Layer), 474
 - IMAP over SSL, 167, 170
 - LDAPS, 167, 171
 - untrusted SSL certificates, troubleshooting, 564
- SSO (Single Sign-On), 429, 478
- SSTP (Secure Socket Tunneling Protocol), 474
- ST (Straight Tip) connectors, 89
- stacks. *See* reference models
- Standard Ethernet, 93, 290
- Standard Operating Procedures (SOP), 386
- standby routers, 312
- star topologies, 45, 50
- state transition modulation, 8–9
- stateful firewalls, 238
- static address assignment, DHCP, 182
- static IP configurations, 120–125
- static routes, 260
- StatTDM (Statistical Time-Division Multiplexing), physical layer (OSI model), 11
- status indicators, LED, troubleshooting, 508
- storage
 - Fibre Channel, 57
 - iSCSI, 57
 - NAS, 43, 57
- store-and-forward networks, 16
- STP (Shielded Twisted Pair) cable, 82–83, 506
- STP (Spanning Tree Protocol), 298–299
 - hardening networks, 456
 - Layer 2 loops, 301
 - nonroot bridges, 301
 - ports
 - costs, 302–303
 - designated ports, 302
 - identifying roles, 302
 - long STP, 303
 - nondesignated ports, 302, 303
 - root ports, 302
 - root bridges, 301
- strategies, exam taking, 576–577
- stratum, NTP, 190
- strippers, cable, 514
- structured troubleshooting methodologies, 498–501
- study mode, final review/study plan, 574
- study/final review plan
 - exam preparation, 574–575
 - flash card mode, 575
 - practice exam mode, 574
 - study mode, 574
- subinterfaces, 120
- subnet masks, 114–116

- 8-bit subnet masks, 114
- classful masks, 115
 - borrowed bits, 133
 - extending, 132–133
- IPv4 addresses, 113
- notation, 130–132
- octets, 131
- VLSM, 130
- subnetting, 129
 - advanced practice exercises, 139–143
 - calculating
 - new IP address ranges, 139
 - number of available hosts, 134
 - number of subnets, 133
 - CIDR, 144
 - classful masks, CIDR, 144
 - Ethernet switches, 293
 - managing IP addresses, 143
 - practice exercises, 134–136
 - purpose of, 129–130
 - screened subnets, 427
 - subet masks, notation, 130–132
 - subnet masks, octets, 131
 - VLSM, 130
- suggested final review/study plan
 - exam preparation, 574–575
 - flash card mode, 575
 - practice exam mode, 574
 - study mode, 574
- suplicants, 310, 430, 477
- surfing, shoulder, 445
- Switch Book, The*, 5
- switching, 222
 - broadcast domains, 293
 - circuit switching, network layer (OSI model), 15
 - collisions, 230–231
 - end-of-rack switching, 204
 - Ethernet, 292
 - 802.1Q standard (dot1q), 297
 - 802.1X user authentication, 309–310
 - access management, 311–312
 - access ports, 295
 - authentication, 311–312
 - broadcast storms, 300–301
 - case studies, 314–315
 - collision domains, 289
 - connectors, 291
 - diagnostics, 313–314
 - first-hop redundancy, 312–313
 - link aggregation, 304–305
 - MAC address table corruption, 299
 - packet capturing, 307–309
 - PoE, 306–307
 - PoE+, 307
 - port mirroring, 307–309
 - port monitoring, 307–309
 - port tagging, 297
 - QoS, 314
 - RSTP, 298
 - Shortest Path Bridging, 299
 - STP, 298–299, 301–303
 - subnets, 293
 - trunks, 296–297
 - VLAN, 293–295
 - Layer 2 switches, 225–231, 234, 243
 - Layer 3 capable switches, 231–232, 234, 243
 - magnetic door switches, 246
 - MDI-X technology, 297
 - message switching, network layer (OSI model), 16
 - multilayer switches, 231–232, 234, 243
 - network layer (OSI model), 15–16
 - packet switching/routing, network layer (OSI model), 15
 - top-of-rack switching, 204
 - unneeded ports, disabling, 455
 - vSwitches, 58–59
- switching, content, 401–402
- switching loops, troubleshooting, 565
- symmetric encryption, 419–420, 422
- SYN flooding, 448
- synchronization
 - asynchronous synchronization, 10
 - bits, 9
 - synchronous synchronization, 10
 - transmissions
 - asynchronous transmissions, 14
 - isynchronous transmissions, 13
 - LLC, 13–14
 - synchronous transmissions, 14

- Syslog, 169, 172
 - clients, 361
 - message structure, 362
 - security, 361–362
 - servers, 361, 363
 - system life cycles, 377–378
 - system logs, 364
- T**
- T connectors, bus topologies, 46–47
 - T1 circuits, 66
 - T3 circuits, 67
 - tables, memory tables, exam preparation, 572–573
 - TACACS+ (Terminal Access Controller Access Control System Plus), 429, 477
 - tagging, 297
 - tags, asset tracking, 486
 - tailgating, 445
 - tamper detection, 486
 - TAP (Traffic Access Points), 513
 - targets, iSCSI, 57
 - $Tc = Bc / CIR$ formula, 276
 - TCP (Transmission Control Protocol), 172, 174
 - flags, 25
 - flooding, 448
 - ports, blocked ports, troubleshooting, 564
 - segment format, transport layer (TCP/IP stack), 24–25
 - sliding windows, 18
 - transport layer (OSI model), 17
 - tcpdump command, 542
 - TCP/IP protocol suite (summary), 173–175
 - TCP/IP stack, 22, 25
 - application layer, 25
 - application protocols, 26–27
 - Internet layer, 23
 - IP addresses, 26–27
 - layers of (overview), 22–25
 - network interface layer, 22
 - port numbers, 26–27
 - transport layer, 24–25
 - TDM (Time-Division Multiplexing), 10, 68
 - TDR (Time-Domain Reflectometers), 511–512
 - teaming, NIC, 397
 - technology-based attacks
 - ARP spoofing, 442
 - botnets, 441
 - brute-force password attacks, 443
 - command and control software, 441
 - DDoS attacks, 441
 - deauthentication attacks, 444
 - dictionary password attacks, 443
 - DNS poisoning, 442
 - DoS attacks, 440–441
 - evil twins (rogue AP), 443
 - IP spoofing, 444
 - MAC spoofing, 444
 - malware, 444–445
 - Man-in-the-Middle (MitM) attacks.
 - See on-path attacks
 - password attacks, 443
 - on-path attacks, 441
 - ransomware, 443
 - rogue AP, 443
 - VLAN hopping, 442
 - zombies, 441
 - Telnet, 170, 172, 174
 - temperature, network availability, 354
 - Terminal Access Controller Access Control System Plus (TACACS+), 429, 477
 - terminal emulators, 522
 - testing
 - cable testers, 513
 - penetration testing, 432
 - theories of probable cause, troubleshooting, 499
 - tethering, 333
 - TFA (Two-Factor Authentication), 478
 - TFTP (Trivial File Transfer Protocol), 170, 172, 174, 522
 - theories of probable cause
 - establishing, 499
 - testing, 499
 - thicknet, 90, 284
 - thinnet, 91, 284
 - threats, 423, 431

- three-tiered network architectures, 198
 - access/edge layer, 198–199
 - core layer, 200
 - distribution/aggregation layer, 199–200
- throughput
 - cabling, 506
 - WLAN deployments, troubleshooting, 550
- TIA/EIA-568 standard, twisted-pair cable, 82
- TIA/EIA-568-B Wiring Standard, RJ-45 connectors, 9
- tickets, trouble, 496
- time (incorrect), troubleshooting, 564
- time slots, 10
- timers, hold-down, 265
- TKIP (Temporal Key Integrity Protocol), 344
- TLS (Transport Layer Security), 175, 474
- Token Ring topologies, 286
- tone generators, 510
- tools
 - cabling tools, 509–514
 - command line tools, 522, 537
 - arp command, 533–535
 - case studies, 543
 - dig command, 531–532
 - ifconfig command, 528–529
 - ip command, 529
 - ipconfig command, 524–528
 - ipconfig/all command, 526–527
 - ipconfig/release command, 527–528
 - netstat command, 535–537
 - nmap command, 542
 - nslookup [fqdn] command, 529–531
 - nslookup command, 529, 531
 - ping command, 523–524
 - route add command, 541–542
 - route command, 538–542
 - route delete command, 540–541
 - route print command, 538–540
 - tcpdump command, 542
 - traceroute command, 532–533
 - end-of-chapter review tools, 573
 - exam preparation, 571–572
 - network platform commands, 543
 - software tools, 520
 - bandwidth speed testers, 520
 - case studies, 543
 - collectors, 522
 - IP scanners, 521, 522
 - iperf, 521–522
 - NetFlow analyzers, 522
 - network sniffers, 520–521
 - packet capturing, 520–521
 - port scanners, 521
 - protocol analyzers, 520–521
 - terminal emulators, 522
 - TFTP servers, 522
 - WiFi analyzers, 520
- top-of-rack switching, 204
- topologies
 - ADSL, 62–63
 - bus topologies, 46–48, 286
 - cable modems, 64
 - content engines, 401
 - content switching, 401–402
 - demarcation points, 55
 - full-mesh topologies, 52–53
 - HSRP, 312–313
 - hub-and-spoke topologies, 51–52
 - hybrid networks, 54
 - LACP, 399
 - logical topologies
 - MAC, 13
 - physical topologies versus, 45–46
 - mesh topology, WLAN, 336
 - NAT, 145–146
 - partial-mesh topologies, 53–54
 - PAT, 148
 - physical topologies
 - logical topologies versus, 45–46
 - physical layer (OSI model), 9
 - ring topologies, 46, 48–49
 - routing, 256
 - service-related entry points, 55
 - SOHO network design, 403–404, 410
 - spine and leaf topologies, 202–204
 - star topologies, 45, 50
 - Token Ring topologies, 286
 - VoIP network topologies, 244
- top-to-bottom troubleshooting, 499
- traceroute command, 532–533

- tracking tags, 486
- traffic
 - best-effort treatment, 273
 - $CIR = Bc / Tc$ formula, 276
 - conforming, 276
 - exceeding, 276
 - Low Priority traffic, 273
 - policing, 275–276
 - priority treatment, 273
 - send/receive traffic statistics/statuses, 366
 - shaping, 275–276
 - $Tc = Bc / CIR$ formula, 276
- traffic flows, 201–202
- traffic logs, 360
- training
 - employees, prevention methods, 486–487
 - video training, exam preparation, 572
- transceivers, 95
 - Ethernet, 291
 - troubleshooting, 508
- transition modulation, 8–9
- transmission methods, MAC, 13
- transmissions
 - methods of, 330–331
 - spread spectrum transmissions, 330
 - FHSS, 330
 - OFDM, 330
 - OFDMA, 331
 - synchronization
 - asynchronous transmissions, 14
 - isynchronous transmissions, 13
 - LLC, 13–14
 - synchronous transmissions, 14
- transmit (Tx) reads, troubleshooting, 509
- transport layer
 - OSI model, 17
 - buffering, 18
 - ICMP, 19
 - TCP, 17
 - UDP, 17
 - windowing, 18
 - TCP/IP stack, 24–25
- transport mode, ESP, 471
- Trap messages, 357
- Triple Data Encryption Standard (3DES), 419
- trouble tickets, 496
- troubleshooting
 - ACL, 564
 - action plans, 500
 - antennas, 551
 - AP, 554
 - attenuation, 507
 - back-out plans, 500
 - bad cable, 508
 - bad ports, 508
 - basics, 496
 - blocked IP addresses, 564
 - blocked services, 564
 - blocked TCP/UDP ports, 564
 - bottom-to-top troubleshooting, 499
 - broadcast storms, 565
 - BYOD policies, 566
 - cabling, 507
 - attenuation, 507
 - bad cable, 508
 - bad ports, 508
 - decibel (dB) loss, 508
 - dirty optical cables, 509
 - duplexing, 509
 - interference, 508
 - LED status indicators, 508
 - opens, 508
 - pinouts, 508
 - pins, 508
 - receive (Rx) reads, 509
 - shorts, 508
 - speed (data rates), 509
 - transceivers, 508
 - transmit (Tx) reads, 509
 - captive portals, 554
 - case studies, 501, 566–567
 - channels, 552
 - collisions, 565
 - decibel (dB) loss, 508
 - device configurations, 562
 - DHCP, scope exhaustion, 564
 - diagnosing problems, 497
 - dirty optical cables, 509
 - divide-and-conquer troubleshooting, 499
 - duplexing, 509

- duplicate IP addresses, 563
- escalating issues, 500
- expired IP addresses, 564
- firewalls, 564
- frequencies, 552
- full system functionality, verifying, 500
- fundamentals, 496–497
- identifying problems, 499
- implementing solutions, 500
- incorrect time, 564
- interface status, 562–563
- interference, 508, 553
- IP addressing
 - blocked addresses, 564
 - duplicate IP addresses, 563
 - expired IP addresses, 564
- latency (delay), 553
- LED status indicators, 508
- licensed features, 566
- loss budgets, 566
- low optical link budgets, 566
- multicast flooding, 565
- networks, 562
 - ACL, 564
 - asymmetrical routing, 565
 - blocked IP addresses, 564
 - blocked services, 564
 - blocked TCP/UDP ports, 564
 - broadcast storms, 565
 - BYOD policies, 566
 - collisions, 565
 - device configurations, 562
 - DHCP scope exhaustion, 564
 - duplicate IP addresses, 563
 - duplicate MAC addresses, 563
 - expired IP addresses, 564
 - firewalls, 564
 - hardware failures, 566
 - incorrect time, 564
 - interface status, 562–563
 - licensed features, 566
 - loss budgets, 566
 - low optical link budgets, 566
 - missing routes, 566
 - multicast flooding, 565
 - performance, 566
 - performance baselines, 563
 - rogue DHCP servers, 564
 - routing loops, 565
 - routing tables, 562
 - switching loops, 565
 - TCP ports, 564
 - UDP ports, 564
 - unresponsive services, 565
 - untrusted SSL certificates, 564
 - VLAN, 563
- opens, 508
- optical cables (dirty), 509
- performance, networks, 566
- pinouts, 508
- pins, 508
- postmortem reports, 501
- preventive measures, implementing, 500
- propagation paths, 554
- receive (Rx) reads, 509
- routing tables, 562
- services, blocked services, 564
- shorts, 508
- signal strength, 553
- simplified troubleshooting flow, 497
- speed (data rates), 509
- SSL certificates, 564
- status indicators, LED, 508
- structured troubleshooting methodologies, 498–501
- TCP, blocked ports, 564
- theories of probable cause
 - establishing, 499
 - testing, 499
- time, 564
- top-to-bottom troubleshooting, 499
- transceivers, 508
- transmit (Tx) reads, 509
- trouble tickets, 496
- UDP, blocked ports, 564
- untrusted SSL certificates, 564
- wireless networks, 555
- wireless parameter misconfigurations, 553
- WLAN
 - antennas, 551

- AP placement, 554
 - association times, AP, 552
 - captive portals, 554
 - case studies, 556
 - channels, 552
 - client disassociation issues, 554
 - frequencies, 552
 - latency (delay), 553
 - propagation paths, 554
 - signal strength, 553
 - site surveys, 552
 - throughput, 550
 - wireless parameter misconfigurations, 553
 - wrong time, 564
 - trunks
 - connections, 295
 - Ethernet switches, 296–297
 - trust relationship exploitation, 448
 - TTL (Time to Live)
 - DNS TTL, 189
 - IP addressing, 257–258
 - tunnel mode, ESP, 471
 - tunneling
 - child tunnels, 473
 - GRE tunneling, 471
 - IPsec, 470
 - IPv6 addresses, 149
 - L2TP, 474
 - PPTP, 474
 - Q-in-Q tunneling, 442
 - SSTP, 474
 - twinaxial cables, 81
 - twisted-pair cable, 82
 - DB-9 (RS-232) connectors, 85–86
 - RJ11 connectors, 85–86
 - RJ45 connectors, 85–86
 - STP cable, 82–83, 506
 - TIA/EIA-568 standard, 82
 - UTP cable, 83–85, 92–93, 506
 - Cat 5 cable, 83
 - Cat 5e cable, 84
 - Cat 6 cable, 84
 - Cat 6a cable, 84
 - Cat 7 cable, 84
 - Cat 8 cable, 84
 - Two-Factor Authentication (TFA), 478
 - TXT records, DNS, 188
- ## U
- UDP (User Datagram Protocol), 172, 174
 - NTP, 190
 - ports (blocked), troubleshooting, 564
 - transport layer (OSI model), 17
 - UDP segment format, transport layer (TCP/IP stack), 25
 - UNC (Universal Naming Convention), IP addressing, 119
 - underlays, 37
 - Understanding (MOU), Memorandum of, 387
 - unicast IP addresses, 116–117, 152
 - unidirectional antennas, 326, 551
 - unnecessary switch ports, disabling, 455
 - unresponsive services, troubleshooting, 565
 - untrusted SSL certificates, troubleshooting, 564
 - UPC (Ultra Physical Contact), fiber-optic cable, 90
 - updating, 454
 - upgrading firmware, 454–455
 - UPS (Uninterruptible Power Supplies), 400
 - upstream data frequencies, 65
 - uptime (network availability)
 - case studies, 368, 410–411
 - content caching, 401
 - environmental monitors, 354, 365
 - HA, 394
 - backups, 400
 - best practices, 400–401
 - design considerations, 399–400
 - fault-tolerant network design, 395–396
 - hardware redundancy, 397
 - Layer 3 redundancy, 398–399
 - measuring, 394
 - MTBF, 394
 - MTTF, 394
 - MTTR, 394
 - RPO, 395
 - RTO, 395

- SLA, 394
- hardware redundancy, 402–403
- interface statistics/statuses, 367
 - CRC, 367
 - encapsulation errors, 367
 - giants, 367
 - link-state, 366
 - packet byte counts, 367
 - protocol byte counts, 367
 - send/receive traffic, 366
 - speed/duplex, 366
 - viewing, 365–366
- load balancing, 401–402
- logs, 363
 - application logs, 363
 - audit logs, 361
 - Event Viewer logs, 360
 - reviews, 360
 - security logs, 364
 - syslog, 361–363
 - system logs, 364
 - traffic logs, 360
- NetFlow, 368
- performance metrics, 354
 - bandwidth, 355
 - baselines, 356
 - CPU usage, 354
 - jitter, 355
 - latency (delay), 355
 - memory, 355
 - temperature, 354
- SNMP, 356
 - community strings, 357–358
 - Get messages, 357
 - MIB, 356–357
 - OID, 357
 - security, authentication, 359
 - security, authNoPriv, 358
 - security, authPriv, 358
 - security, encryption, 359
 - security, integrity, 359
 - security, levels, 358
 - security, models, 358
 - security, noAuthNoPriv, 358
 - Set messages, 357
 - SNMP agent, 356
 - SNMP manager, 356
 - SNMPv1, 357–358, 359
 - SNMPv2c, 357–358, 359
 - SNMPv3, 358–360
 - Trap messages, 357
 - walks, 357
- SOHO network design, 403
 - cost savings, 409
 - environmental factors, 409
 - fire suppression systems, 409
 - HVAC, 409
 - IP addressing, 405–406
 - Layer 1 media, 406–407
 - Layer 2 devices, 407–408
 - layer 3 devices, 408
 - PDU, 409
 - performance, 409
 - scenario, 403–405
 - suggested solution, 405
 - topologies, 403–404, 410
 - wireless design, 408–409
- URL (Uniform Resource Locators), 189
- usernames
 - common usernames, 454
 - NIST Digital Identity Guidelines, 454
- users
 - 802.1X user authentication, 309–310, 342–343, 430, 477
 - NDA, 385
 - onboarding/offboarding procedures, 384
 - permissions, 426
 - PUA, 383
 - SOP, 386
- UTP (Unshielded Twisted Pair) cable, 83–85, 506
 - 10BASE-T cable standard, 92–93
 - 10BASE-T Ethernet standard, 285–286
 - Cat 5 cable, 83
 - Cat 5e cable, 84
 - Cat 6 cable, 84
 - Cat 6a cable, 84
 - Cat 7 cable, 84
 - Cat 8 cable, 84

V

- variable delay, 271
- VDSL (Very High Bit-Rate DSL), 64
- vendor assessments, 433
- verifying, full system functionality, 500
- video
 - Low Delay, 273
 - QoS, 272
 - training, exam preparation, 572
- viewing interface statistics/statuses, 365–366
- VIP (Virtual IP) addresses, 120
- virtual desktops, 58–60, 476
- virtual firewalls, 58
- virtual networks, 55
 - off-site options, 60
 - on-site options, 60
 - virtual desktops, 58–60
 - virtual firewalls, 58
 - virtual routers, 58
 - virtual servers, 55–57
 - VNC, 476
 - vSwitches, 58–59
- virtual routers, 58
- virtual servers, 55–57
- VLAN (Virtual Local Area Networks)
 - 802.1Q standard (dot1q), 297
 - ARP, 293
 - assigning, troubleshooting, 563
 - default VLAN, changing, 457
 - Ethernet switches, 293–295
 - hopping, 442
 - NDP, 293
 - port tagging, 297
 - private VLAN, 456
 - segmentation, 456
 - trunks, 296–297
 - voice VLAN, 295
 - VTP, trunks, 295
- VLSM (Variable Length Subnet Masking), 130
- VM (Virtual Machines), east-west traffic flows, 202
- VNC (Virtual Network Computing), 476
- vNIC (virtual NIC), 56–57
- voice
 - gateways, 244
 - Low Delay, 273
 - QoS, 272
 - VLAN, 295
- VoIP (Voice over IP)
 - call agents, 245
 - components of, 244–245
 - gateways, 245
 - IP phones, 244
 - network topologies, 244
 - PBX, 245
 - protocols, 244–245
 - RTP, 245
 - SIP, 245
 - voice gateways, 244
- VPN (Virtual Private Networks), 215
 - clientless VPN, 468
 - client-to-site VPN, 466
 - concentrators, 236–237, 243
 - DMVPN, mGRE, 41
 - full tunnel configurations, 468
 - headends, 236–237
 - L2F, 474
 - L2TP, 474
 - OpenVPN, 474
 - PPTP, 474
 - remote access, 466
 - clientless VPN, 468
 - client-to-site VPN, 466
 - site-to-site VPN, 466–467
 - site-to-site VPN
 - IPsec site-to-site VPN setup/tear down, 472–473
 - remote access, 466–467
 - split tunnel configurations, 468
 - SSL, 474
 - SSTP, 474
 - TLS, 474
- VRRP (Virtual Router Redundancy Protocol), 313, 398
- vSwitches, 58–59
- VTP (VLAN Trunking Protocol), trunks, connections, 295
- VTY lines, 312
- vulnerabilities, 423–424, 432

W

Walking Dead, The, 441

walks, SNMP, 357

WAN (Wide Area Networks)

 MPLS, 40–41

 sample topology, 38

 satellite provider links, 60–62

 SD-WAN, 39–40

WAP (Wireless Access Points), 234, 323–324

 interference, 552

 placement of, 338–339

war chalking, 339–340

war dialing, 339

war driving, 339

war flying, 340

warm sites, 402

WDM (Bidirectional Wavelength-Division Multiplexing), 96

weather sensitivity, satellite provider links, 61–62

well-known ports, 27

WEP (Wired Equivalent Privacy), 340, 343–344

Wi-Fi 4 (802.11n) wireless standard, 332, 333

Wi-Fi 5 (802.11ac) wireless standard, 332, 333

Wi-Fi 6 (802.11ax) wireless standard, 327, 332, 333

WiFi analyzers, 520

windowing

 TCP sliding windows, 18

 transport layer (OSI model), 18

wipe configurations, 489

wire maps, 513

wireless bands, 332

wireless channels, 327

wireless client isolation, 458

wireless design, SOHO network design, 408–409

wireless networks, troubleshooting, 555

wireless parameters, troubleshooting misconfigurations, 553

wireless routers, 322–323

wireless security, 458–459

wireless security system devices, RFI, 337

wireless standards

 802.11, 333

 802.11a, 331, 333

 802.11ac (Wi-Fi 5), 332, 333

 802.11ax (Wi-Fi 6), 332, 333

 802.11b, 331, 333

 802.11g, 331, 333

 802.11n (Wi-Fi 4), 332, 333

 case studies, 345–346

wiretapping, 446

wiring closets, 96

wiring diagrams, 386

wiring standards

 connectors, 9

 jacks, 9

WLAN (Wireless Local Area Networks), 38, 321–322, 550

 802.11 wireless standard, 333

 802.11a wireless standard, 331, 333

 802.11ac (Wi-Fi 5) wireless standard, 332, 333

 802.11ax (Wi-Fi 6) wireless standard, 332, 333

 802.11b wireless standard, 331, 333

 802.11g wireless standard, 331, 333

 802.11n (Wi-Fi 4) wireless standard, 332, 333

ad hoc WLAN, 322, 334

antennas, 324

 design goals, 324–325

 gain, 325

 omnidirectional antennas, 325–326

 polarity, 326

 unidirectional antennas, 326

associations, 323

BSS WAN, 334, 335

case studies, 345–346

cells, 338

cellular technologies, 333–334

channels, 327–329

 honeycomb channels, 339

 nonoverlapping channels, 338–339

components of, 322

concepts, 322

CSMA/CA, 329

deploying, 334–339

- ESS WLAN, 334
 - frequencies, 327–329, 338–339
 - honeycomb channels, 339
 - hotspots, 322
 - IBSS WLAN, 322, 334
 - infrastructure mode, 335
 - interference, 336–337
 - mesh topology, 336
 - nonoverlapping channels, 338–339
 - RFI, 336–337
 - security, 339
 - 802.1X user authentication, 342–343
 - EAP, 343
 - ESSID, 341
 - geofencing, 345
 - issues, 339–341
 - MAC address filtering, 341
 - open authentication, 341
 - Personal mode, 341–342
 - RADIUS, 342
 - RC4 encryption, 343–344
 - rogue AP, 340
 - SSID, 340–341
 - SSID, disabling broadcasts, 341
 - standards (overview), 343
 - war chalking, 339–340
 - war dialing, 339
 - war driving, 339
 - war flying, 340
 - WEP, 340, 343–344
 - WEP security cracking,
 - WPA, 340, 344
 - WPA2, 345
 - WPA3, 342
 - transmission methods, 330–331
 - troubleshooting, 550
 - antennas, 551
 - AP placement, 554
 - association times, AP, 552
 - captive portals, 554
 - case studies, 556
 - channels, 552
 - client disassociation issues, 554
 - distance (attenuation), 550
 - EIRP/power settings, 551
 - frequencies, 552
 - interference, 553
 - latency (delay), 553
 - propagation paths, 554
 - RSSI signal strength, 550
 - site surveys, 552
 - speed (data rates), 550
 - throughput, 550
 - wireless parameter misconfigurations, 553
 - WAP, 323–324, 338–339
 - wireless routers, 322–323
 - WLC (Wireless LAN Controllers), 235, 243, 324
 - work instructions, 386
 - WPA (Wi-Fi Protected Access), 340, 344
 - WPA2, 345
 - WPA3, 342
 - WPAN (Wireless PAN), 39
 - wrong time, troubleshooting, 564
- X**
- XaaS (Everything as a Service), 213
 - Xerox Corporation, Ethernet, 284
- Y - Z**
- Zero Trust security, 426
 - Zeroconf (Zero Configuration), 129
 - zero-day attacks, 424
 - zombies, 441
 - zone transfers, DNS, 189
 - Z-Wave, 247