

PEARSON IT

CYBERSECURITY CURRICULUM



SIXTH EDITION

NETWORKING ESSENTIALS

A CompTIA® Network+ N10-008 Textbook

Save 10%
on Exam
Voucher

See Inside

JEFFREY S. BEASLEY
PIYASAT NILKAEW

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



NETWORKING ESSENTIALS:
SIXTH EDITION
A COMPTIA NETWORK+ N10-008
TEXTBOOK

INSTRUCTOR EDITION

JEFFREY S. BEASLEY AND PIYASAT NILKAEW



Networking Essentials: Sixth Edition

Instructor Edition

Copyright © 2022 by Pearson Education, Inc.

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: 978-0-13-745582-9

ISBN-10: 0-13-745582-8

Library of Congress Control Number: 2021913557

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.

Warning and Disclaimer

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

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.

EDITOR-IN-CHIEF

Mark Taber

DIRECTOR, ITP PRODUCT MANAGEMENT

Brett Bartow

DEVELOPMENT EDITOR

Marianne Bartow

MANAGING EDITOR

Sandra Schroeder

PROJECT EDITOR

Mandie Frank

COPY EDITOR

Kitty Wilson

INDEXER

Ken Johnson

PROOFREADER

Abigail Manheim

TECHNICAL EDITOR

Chris Crayton

PEER REVIEWERS

DeAnnia Clements

Osman Guzide

Gene Carwile

Dr. Theodor Richardson

PUBLISHING COORDINATOR

Cindy Teeters

DESIGNER

Chuti Prasertsith

COMPOSITOR

codeMantra

CREDITS

- Figure 1-8** Screenshot of The command prompt in Windows 10 © Microsoft 2020
- Figure 1-9** Screenshot of A typical text screen result when entering the ipconfig /all command in the command window. © Microsoft 2020
- Figure 1-15** courtesy for Linksys
- Figure 1-18** courtesy Zoom Telephonics, Inc.
- Figure 1-19** courtesy for Linksys
- Figure 1-27** Screenshot of (a) An example of displaying the IP address for computer 1 using the ipconfig command in Windows and (b) an example of the displayed IP address in macOS for the built-in Ethernet connection © Microsoft 2020
- Figure 2-34** Screenshot of DTX-1800 certification report: Failure due to a termination problem. ©Fluke Corporation
- Figure 2-35** Screenshot of DTX-1800 certification report: Failure due to excessive insertion loss. ©Fluke Corporation
- Figure 2-36** Screenshot of The certification report for Test 1, showing that a short jumper cable passes the CAT5e link test. ©Fluke Corporation
- Figure 2-37** Screenshot of The results for Test 2, showing that the cable failed the CAT5e link test. ©Fluke Corporation
- Figure 2-38** Screenshot of The Test 3 CAT5e link test, showing failures with attenuation. ©Fluke Corporation
- Figure 2-39** Screenshot of A CAT5e link test, showing failures with delay skew (Test 4). ©Fluke Corporation
- Unnumbered**
- Figure 2-1** Screenshot of Answer the following questions related to the certification report shown here. ©Fluke Corporation
- Unnumbered**
- Figure 2-2** Screenshot of Answer the following questions related to the certification report shown here. ©Fluke Corporation
- Unnumbered**
- Figure 2-3** Screenshot of Answer the following questions related to the certification report shown here - OMNI Scanner. ©Fluke Corporation
- Figure 4-7** Screenshot of An example of the information displayed when an association is formed between a client and an access point. © Microsoft 2020
- Figure 4-8** Screenshot of An example of a lost association. © Microsoft 2020
- Figure 4-18** Screenshot of The window for configuring Bluetooth settings on a Mac. © 2020 Apple Inc
- Figure 4-19** Screenshot of The Mac window showing the settings for a file transfer. © 2020 Apple Inc
- Figure 4-20** Screenshot of The Mac window showing that a text file is coming in from another Bluetooth device. © 2020 Apple Inc
- Figure 4-28** Screenshot of The excellent signal quality measured for the multipoint distribution. © Microsoft 2020
- Figure 4-29** Screenshot of The poor signal quality measured at the remote site near the lake. © Microsoft 2020
- Figure 5-7** Screenshot of The data traffic captured by computer 2 for the LAN using a hub. © Microsoft 2020
- Figure 5-8** Screenshot of The data traffic captured by computer 2 for the LAN using a switch. © Microsoft 2020
- Figure 5-9** Screenshot of The startup menu of a Cisco Catalyst switch in the CNA software. © Microsoft 2020
- Figure 5-10** Screenshot of The highlighted ports showing the current connections and the location of the stacked switches icon. © Microsoft 2020
- Figure 5-11** Screenshot of The window listing the MAC addresses currently connected to a switch. © Microsoft 2020
- Figure 5-13** Screenshot of Configuring an IP address on an interface. © Microsoft 2020
- Figure 5-19** Screenshot of Putty configuration © 1997-2020 Simon Tatham
- Figure 5-20** Screenshot of The HyperTerminal Connect To dialog © 1997-2020 Simon Tatham
- Figure 5-21** Screenshot of The Properties dialogs for configuring the serial port connection PuTTY © 1997-2020 Simon Tatham
- Figure 5-23** Screenshot of The macOS dialog for configuring the settings for the serial interface. © 2020 Apple Inc
- Figure 5-24** Screenshot of The macOS dialog for setting the serial port to PL2303-000. © 2020 Apple Inc
- Figure 5-25** Screenshot of The macOS window listing the serial communication link settings. © 2020 Apple Inc
- Figure 6-6** Screenshot of An example of the three packets exchanged in the initial TCP handshake. © Microsoft 2020
- Figure 6-8** Screenshot of An example of the four-packet TCP connection termination. © Microsoft 2020
- Figure 6-10** Screenshot of An example of a UDP packet transfer. © Microsoft 2020
- Figure 6-12** Screenshot of Captured packets showing the (a) ARP request and the (b) ARP reply. © Microsoft 2020
- Figure 6-13** Screenshot of The details of the ARP broadcast packet. © Microsoft 2020
- Figure 6-14** Screenshot of An example of the use of hex numbers in data packets. © Microsoft 2020
- Figure 7-3** Screenshot of The TCP/IP dialog for setting the default gateway address for computer A1. © Microsoft 2020
- Figure 7-6** Screenshot of The Net-Challenge screen. © Microsoft 2020
- Figure 7-7** Screenshot of The check box window for the Net-Challenge software User EXEC Mode challenge. © Microsoft 2020

Figure 7-8	Screenshot of The display for step 6, using the show command. © Microsoft 2020
Figure 7-11	Screenshot of The network topology for Net-Challenge. The arrows indicate where to click to display the router IP address configurations. © Microsoft 2020
Figure 7-14	Screenshot of An example of the port management options available with a Cisco switch: (a) Speed auto-negotiation option; (b) Duplex auto option. © Microsoft 2020
Figure 9-1a	Screenshot of Setting the default gateway address or default static route on a host computer (PC). © Microsoft 2020
Figure 9-1b	Screenshot of Setting the default gateway address or default static route on a host computer (macOS). © Microsoft 2020
FIG10-4	Screenshot of Captured DHCP packets. © Microsoft 2020
FIG10-9	Screenshot of An example of using an SNMP software management tool to obtain descriptions of a router's interfaces using the MIB ifDescr. © Microsoft 2020
FIG10-11	Screenshot of Using an SNMP software management tool to obtain interface speed settings. © Microsoft 2020
FIG10-12	Screenshot of An example of using SNMP to collect data traffic statistics. © Microsoft 2020
FIG10-23	Screenshot of Initializing Wireshark to capture data packets from a network. © Microsoft 2020
FIG10-24	Screenshot of Starting a capture. © Microsoft 2020
FIG10-25	Screenshot of The captured packets showing the ping from computer 1 to computer 2. © Microsoft 2020
FIG10-26	Screenshot of Computer 2 replying to computer 1 with its MAC address. © Microsoft 2020
FIG10-27	Screenshot of Computer 1 is sending an echo request to computer 2. © Microsoft 2020
FIG10-28	Screenshot of The echo reply received by computer 1. © Microsoft 2020
FIG10-30	Screenshot of (a) The beginning of the FTP data packet transfer and the request for an ASCII data transfer by the client. (b) The FTP data packet transfer and the closing of the FTP transfer. © Microsoft 2020
FIG10-31	Screenshot of Figure for problems 64–68. © Microsoft 2020
FIG11-9	Screenshot of Windows Firewall in Windows 10. © Microsoft 2020
FIG11-10	Screenshot of Windows 10 Firewall status. © Microsoft 2020
FIG11-11	Screenshot of Windows 10 allowed apps. © Microsoft 2020
FIG11-12	Screenshot of Windows 10 advanced firewall settings. © Microsoft 2020
FIG11-13	Screenshot of Windows 10 echo request properties. © Microsoft 2020
FIG11-14	Screenshot of Windows 10 echo request protocols and ports. © Microsoft 2020
FIG11-15	Screenshot of macOS firewall. © 2020 Apple Inc
FIG11-16	Screenshot of macOS advanced settings. © 2020 Apple Inc
FIG11-17	Screenshot of Linux iptables © The Netfilter's webmasters
FIG11-19	Screenshot of An example of setting WEP encryption on a wireless client. © Microsoft 2020
FIG11-26	Screenshot of The traceroute from the VPN server to the VPN remote client. © Microsoft 2020
FIG11-27	Screenshot of The first window, the VPN Client status window, is displayed after starting the VPN client software. © Cisco systems
FIG11-28	Screenshot of The connection screen for establishing a VPN link. © Cisco systems
FIG11-29	Screenshot of The initial handshake screen for the VPN client. © Cisco systems
FIG11-30	Screenshot of The menu showing that the VPN client has successfully connected to the virtual private network. © Cisco systems
FIG11-31	Screenshot of The Preferences window for the VPN client. © Cisco systems
FIG11-32	Screenshot of The Statistics window (a) and Route Details window (b) for the VPN client. © Cisco systems
FIG12-1	Screenshot of Enabling Hyper-V © Microsoft 2020
FIG12-2	Screenshot of Using Hyper-V Manager © Microsoft 2020
FIG12-3	Screenshot of Creating a virtual switch in Hyper-V © Microsoft 2020
FIG12-4	Screenshot of Specifying the name of a virtual switch © Microsoft 2020
FIG12-5	Screenshot of Creating a virtual machine © Microsoft 2020
FIG12-6	Screenshot of Specifying the name and location of a virtual machine. © Microsoft 2020
FIG12-7	Screenshot of Specifying the generation of the virtual machine © Microsoft 2020
FIG12-8	Screenshot of Specifying the desired memory size for a VM. © Microsoft 2020
FIG12-9	Screenshot of Selecting the connection name of the virtual switch. © Microsoft 2020
FIG12-10	Screenshot of Specifying a virtual hard disk name, location, and size. © Microsoft 2020
FIG12-11	Screenshot of The options for installing the VM's operating system. © Microsoft 2020
FIG12-12	Screenshot of Starting the new VM. © Microsoft 2020
FIG12-13	Screenshot of The final VM screen, showing that the machine is up. © Microsoft 2020
Cover	Peter Mell (NIST), Tim Grance (NIST), The NIST Definition of Cloud Computing, SP 800-145 Artistdesign29/Shutterstock

CONTENTS AT A GLANCE

	Introduction	xxiii
1	Introduction to Computer Networks	2
2	Physical Layer Cabling: Twisted-Pair	62
3	Physical Layer Cabling: Fiber Optics	124
4	Wireless Networking	172
5	Interconnecting the LANs	228
6	TCP/IP	290
7	Introduction to Router Configuration	354
8	Introduction to Switch Configuration	404
9	Routing Protocols	444
10	Managing the Network Infrastructure	524
11	Network Security	590
12	Cloud Computing and Virtualization	676
13	Codes and Standards	706
	Glossary	742
	Index	764

Online Only Elements:

Net-Challenge Software

Wireshark Captures

Network+ quizzes

CONTENTS

Introduction

xxiii

CHAPTER 1	Introduction to Computer Networks	2
	Chapter Outline	3
	Objectives	3
	Key Terms	3
1-1	Introduction	4
1-2	Network Topologies	6
	Section 1-2 Review	11
	Test Your Knowledge	11
1-3	The OSI Model	12
	Section 1-3 Review	15
	Test Your Knowledge	15
1-4	The Ethernet LAN	16
	IP Addressing	20
	Section 1-4 Review	22
	Test Your Knowledge	23
1-5	Home Networking	24
	Securing a Home Network	33
	IP Addressing in a Home Network	34
	Section 1-5 Review	36
	Test Your Knowledge	38
1-6	Assembling an Office LAN	38
	Diagram the Network	39
	Connect the Network Devices	40
	Configure the Computers to Operate on the LAN	44
	Section 1-6 Review	44
	Test Your Knowledge	45
1-7	Testing and Troubleshooting a LAN	45
	Section 1-7 Review	48
	Test Your Knowledge	49
	Summary	50
	Questions and Problems	50
	Certification Questions	59

CHAPTER 2	Physical Layer Cabling: Twisted-Pair	62
	Chapter Outline	63
	Objectives	63
	Key Terms	63
2-1	Introduction	65
2-2	Structured Cabling	66
	Horizontal Cabling	69
	Section 2-2 Review	73
	Test Your Knowledge	73
2-3	Twisted-Pair Cable	74
	Unshielded Twisted-Pair Cable	74
	Shielded Twisted-Pair Cable	76
	Section 2-3 Review	77
	Test Your Knowledge	77
2-4	Terminating Twisted-Pair Cables	78
	Computer Communication	79
	Straight-Through and Crossover Patch Cables	82
	Section 2-4 Review	90
	Test Your Knowledge	91
2-5	Cable Testing and Certification	92
	Section 2-5 Review	96
	Test Your Knowledge	97
2-6	10 Gigabit Ethernet over Copper	97
	Overview	98
	Alien Crosstalk	98
	Signal Transmission	100
	Section 2-6 Review	101
	Test Your Knowledge	101
2-7	Troubleshooting Cabling Systems	102
	Cable Stretching	102
	Cable Failing to Meet Manufacturer Specifications	102
	CAT5e Cable Test Examples	104
	Section 2-7 Review	111
	Test Your Knowledge	111
	Summary	112
	Questions and Problems	112
	Certification Questions	121

Chapter Outline	125
Objectives	125
Key Terms	125
3-1 Introduction	126
3-2 The Nature of Light	129
Graded-Index Fiber	133
Single-Mode Fibers	134
Section 3-2 Review	135
Test Your Knowledge	135
3-3 Fiber Attenuation and Dispersion	136
Attenuation	136
Dispersion	137
Dispersion Compensation	139
Section 3-3 Review	140
Test Your Knowledge	140
3-4 Optical Components	141
Intermediate Components	142
Detectors	143
Fiber Connectorization	145
Section 3-4 Review	146
Test Your Knowledge	147
3-5 Optical Networking	147
Defining Optical Networking	148
Building Distribution	151
Campus Distribution	154
Optical Link Budget	157
Section 3-5 Review	158
Test Your Knowledge	159
3-6 Safety	160
Section 3-6 Review	161
Test Your Knowledge	162
3-7 Troubleshooting Fiber Optics: The OTDR	162
Section 3-7 Review	164
Test Your Knowledge	164
Summary	165
Questions and Problems	165
Certification Questions	169

CHAPTER 4 Wireless Networking

172

Chapter Outline	173
Objectives	173
Key Terms	173
4-1 Introduction	174
4-2 The IEEE 802.11 Wireless LAN Standard	175
Section 4-2 Review	184
Test Your Knowledge	185
4-3 802.11 Wireless Networking	185
Section 4-3 Review	195
Test Your Knowledge	196
4-4 Bluetooth, WiMAX, RFID, and Mobile Communications	197
Bluetooth	197
WiMAX	199
Radio Frequency Identification	200
Mobile (Cellular) Communications	204
Section 4-4 Review	205
Test Your Knowledge	206
4-5 Configuring a Point-to-Multipoint Wireless LAN: A Case Study	206
Step 1: Conducting an Antenna Site Survey	207
Step 2: Establishing a Point-to-Point Wireless Link to the Home Network	208
Steps 3 and 4: Configuring the Multipoint Distribution and Conducting an RF Site Survey	209
Step 5: Configuring the Remote Installations	211
Section 4-5 Review	212
Test Your Knowledge	212
4-6 Troubleshooting Wireless Networks	213
Access Point Hardware Issues	213
Wireless Router Issues	213
Wireless Compatibility	213
Signal Strength Problems	214
Wireless Coverage	214
Extending the Wireless Range	214
Frequency Interference Problems	214
Wireless Channel Utilization	214
Load Issues	215
SSID Issues	215
Securing Wi-Fi Issues	215
Cable Issues	215
Deauthentication/Disassociation Attacks	215

DHCP Issues	216
Wireless Printer Issues	216
Section 4-6 Review	216
Test Your Knowledge	216
Summary	217
Questions and Problems	217
Critical Thinking	224
Certification Questions	224

CHAPTER 5 Interconnecting the LANs 228

Chapter Outline	229
Objectives	229
Key Terms	229
5-1 Introduction	230
5-2 The Network Bridge	232
Section 5-2 Review	236
Test Your Knowledge	237
5-3 The Network Switch	237
Hub and Switch Comparison	239
Managed Switches	242
Multilayer Switches	247
Section 5-3 Review	247
Test Your Knowledge	248
5-4 The Router	249
The Router Interface	250
Quality of Service	251
Section 5-4 Review	253
Test Your Knowledge	254
5-5 The Console Port Connection	254
Configuring the PuTTY Software (Windows)	256
Configuring the ZTerm Serial Communications Software (Mac)	259
Section 5-5 Review	261
Test Your Knowledge	261
5-6 Interconnecting LANs with the Router	262
Gateway Address	265
Network Segments	265
Section 5-6 Review	266
Test Your Knowledge	266

5-7	Interconnecting LANs and WANs	267
	Three-Tiered LAN Architecture	267
	Core	268
	Distribution/Aggregation Layer	269
	Access/Edge Layer	269
	Traffic Flow	269
	Data Center Architecture	269
	WAN High-Speed Serial Connections	270
	Data Channels	270
	Point of Presence	271
	Metro Optical Ethernet/Carrier Ethernet	273
	Ethernet Service Types	274
	Service Attributes	276
	Section 5-7 Review	277
	Test Your Knowledge	277
	Summary	279
	Questions and Problems	279
	Critical Thinking	287
	Certification Questions	287
CHAPTER 6	TCP/IP	290
	Chapter Outline	291
	Objectives	291
	Key Terms	291
6-1	Introduction	292
6-2	The TCP/IP Layers	294
	The Application Layer	295
	The Transport Layer	296
	The Internet Layer	301
	The Network Interface Layer	304
	Section 6-2 Review	304
	Test Your Knowledge	305
6-3	Number Conversion	306
	Binary-to-Decimal Conversion	306
	Decimal-to-Binary Conversion	307
	Hexadecimal Numbers	309
	Converting Hexadecimal	309
	Section 6-3 Review	312
	Test Your Knowledge	312

6-4	IPv4 Addressing	312
	Section 6-4 Review	316
	Test Your Knowledge	316
6-5	Subnet Masks: Subnetting and Supernetting	317
	Subnetting	318
	Alternative Technique to Derive the Subnets: Magic Number	323
	Subnet Masking Examples	324
	Gateway IP Address	326
	Section 6-5 Review	327
	Test Your Knowledge	327
6-6	Supernetting, CIDR Blocks, and VLSM	328
	Section 6-6 Review	332
	Test Your Knowledge	332
6-7	IPv6 Addressing	333
	Transitioning to IPv6	335
	CIDR for IPv6	337
	Section 6-7 Review	338
	Test Your Knowledge	339
	Summary	340
	Questions and Problems	340
	Critical Thinking	349
	Certification Questions	350

CHAPTER 7 Introduction to Router Configuration 354

	Chapter Outline	355
	Objectives	355
	Key Terms	355
7-1	Introduction	356
7-2	Router Fundamentals	358
	Layer 3 Networks	359
	Section 7-2 Review	364
	Test Your Knowledge	365
7-3	The Router's User EXEC Mode (Router>)	366
	The User EXEC Mode	366
	Router Configuration Challenge: User EXEC Mode	369
	Section 7-3 Review	372
	Test Your Knowledge	372
7-4	The Router's Privileged EXEC Mode (Router#)	373
	The hostname Command	374

The enable secret Command	375
Setting the Line Console Passwords	375
FastEthernet Interface Configuration	376
Serial Interface Configuration	377
Router Configuration Challenge: Privileged EXEC Mode	380
Section 7-4 Review	382
Test Your Knowledge	382
7-5 Configuring the Network Interface: Auto-negotiation	383
Auto-negotiation Steps	384
Full-Duplex/Half-Duplex	384
Section 7-5 Review	386
Test Your Knowledge	387
7-6 Troubleshooting the Router Interface	387
Section 7-6 Review	392
Test Your Knowledge	392
Summary	393
Questions and Problems	393
Critical Thinking	399
Certification Questions	400
CHAPTER 8 Introduction to Switch Configuration	404
Chapter Outline	405
Objectives	405
Key Terms	405
8-1 Introduction	406
8-2 Introduction to VLANs	407
Virtual LANs	407
Section 8-2 Review	409
Test Your Knowledge	410
8-3 Introduction to Switch Configuration	410
Hostname	411
Enable Secret	412
Setting the Line Console Passwords	412
Static VLAN Configuration	414
VLAN Subinterfaces	418
Networking Challenge: Switch Configuration	419
Section 8-3 Review	420
Test Your Knowledge	421

8-4	Spanning Tree Protocol	422
	Section 8-4 Review	424
	Test Your Knowledge	425
8-5	Power over Ethernet	425
	Section 8-5 Review	428
	Test Your Knowledge	429
8-6	Troubleshooting the Switch Interface	429
	Section 8-6 Review	434
	Test Your Knowledge	435
	Summary	436
	Questions and Problems	436
	Critical Thinking	440
	Certification Questions	441

CHAPTER 9 Routing Protocols 444

	Chapter Outline	445
	Objectives	445
	Key Terms	445
9-1	Introduction	446
9-2	Static Routing	447
	Gateway of Last Resort	454
	Configuring Static Routes	454
	Networking Challenge: Static Routes	458
	Section 9-2 Review	458
	Test Your Knowledge	459
9-3	Dynamic Routing Protocols	460
	Section 9-3 Review	462
	Test Your Knowledge	463
9-4	Distance Vector Protocols	463
	Section 9-4 Review	465
	Test Your Knowledge	466
9-5	Configuring RIP and RIPv2	466
	Configuring Routes with RIP	468
	Configuring Routes with RIPv2	473
	Networking Challenge: RIPv2	474
	Section 9-5 Review	475
	Test Your Knowledge	476
9-6	Link State Protocols	476
	Section 9-6 Review	480

Test Your Knowledge	480
9-7 Configuring the Open Shortest Path First (OSPF) Routing Protocol	481
Networking Challenge: OSPF	485
Section 9-7 Review	486
Test Your Knowledge	487
9-8 Advanced Distance Vector Protocol: Configuring Enhanced Interior Gateway Routing Protocol (EIGRP)	487
Configuring Routes with EIGRP	488
Networking Challenge: EIGRP	494
Section 9-8 Review	495
Test Your Knowledge	495
9-9 Internet Routing with Border Gateway Protocol (BGP)	496
Configuring BGP	496
Section 9-9 Review	498
Test Your Knowledge	498
9-10 IPv6 Routing	499
IPv6 Static Routing	499
RIP for IPv6	499
OSPF for IPv6	500
EIGRP for IPv6	501
BGP for IPv6	501
Section 9-10 Review	502
Test Your Knowledge	503
Summary	504
Questions and Problems	504
Critical Thinking	520
Certification Questions	520
CHAPTER 10 Managing the Network Infrastructure	524
Chapter Outline	525
Objectives	525
Key Terms	525
10-1 Introduction	527
10-2 Domain Name and IP Address Assignment	528
Section 10-2 Review	531
Test Your Knowledge	531
10-3 IP Address Management with DHCP	531
The DHCP Data Packets	534
DHCP Deployment	535

	Section 10-3 Review	537
	Test Your Knowledge	537
10-4	Scaling a Network with NAT and PAT	537
	Section 10-4 Review	539
	Test Your Knowledge	539
10-5	Domain Name System (DNS)	539
	DNS Resource Records	541
	Section 10-5 Review	546
	Test Your Knowledge	546
10-6	Network Management Protocols	546
	Configuring SNMP	547
	Section 10-6 Review	551
	Test Your Knowledge	552
10-7	Analyzing Network Traffic	552
	Section 10-7 Review	559
	Test Your Knowledge	559
10-8	Network Analyzer: Wireshark	560
	Downloading and Installing Wireshark	560
	Using Wireshark to Capture Packets	561
	Using Wireshark to Inspect Data Packets	562
	Section 10-8 Review	565
	Test Your Knowledge	565
10-9	Analyzing Computer Networks: FTP Data Packets	566
	Section 10-9 Review	567
	Test Your Knowledge	567
10-10	Troubleshooting IP Networks	568
	Verifying Network Settings	570
	Investigating IP Address Issues	570
	Finding Subnet Mask Issues	570
	Looking for Gateway Issues	571
	Identifying Name Resolution Issues	571
	Investigating DHCP Issues	571
	Checking for Blocked TCP/UDP Ports	573
	Section 10-10 Review	573
	Test Your Knowledge	573
	Summary	574
	Questions and Problems	574
	Certification Questions	587

CHAPTER 11	Network Security	590
	Chapter Outline	591
	Objectives	591
	Key Terms	591
11-1	Introduction	592
11-2	Intrusion: How Attackers Gain Control of a Network	594
	Social Engineering	595
	Password Cracking	596
	Packet Sniffing	597
	Packet Sniffing Attacks	598
	Vulnerable Software	599
	Preventing Vulnerable Software Attacks	600
	Malware	602
	Section 11-2 Review	604
	Test Your Knowledge	605
11-3	Denial-of-Service	606
	Distributed Denial-of-Service Attacks	608
	Section 11-3 Review	609
	Test Your Knowledge	609
11-4	Security Software and Hardware	610
	Personal Firewalls	610
	Antivirus/Anti-malware Software	610
	Configuring Firewall Settings for Windows 10	611
	Configuring Firewall Settings for macOS	615
	Configuring Firewall Settings for Linux	616
	Firewalls	617
	Other Security Appliances	619
	Computer Forensics	621
	Section 11-4 Review	622
	Test Your Knowledge	622
11-5	Managing Network Access	623
	Section 11-5 Review	625
	Test Your Knowledge	625
11-6	Router Security	626
	Router Access	626
	Router Services	628
	Logging	630
	Section 11-6 Review	631
	Test Your Knowledge	631

11-7	Switch Security	631
	Switch Port Security	633
	Dynamic ARP Inspection	635
	STP Special Features	635
	Section 11-7 Review	637
	Test Your Knowledge	637
11-8	Wireless Security	637
	Section 11-8 Review	641
	Test Your Knowledge	642
11-9	Remote Access and VPN Technologies	642
	Analog Modem Technologies	643
	Cable Modems	644
	xDSL Modems	644
	Remote Access Server	647
	Virtual Private Network	647
	VPN Tunneling Protocols	648
	Configuring a Remote Client's VPN Connection	652
	Configuring a Windows 10 VPN Client	652
	Configuring a macOS VPN Client	652
	Configuring a Cisco VPN Client	653
	Section 11-9 Review	658
	Test Your Knowledge	658
11-10	Physical Security	659
	Access Control Hardware	660
	Detection Methods	661
	Asset Disposal	662
	Internet of Things (IoT) Security Devices	662
	Section 11-10 Review	663
	Test Your Knowledge	663
	Summary	664
	Questions and Problems	664
	Critical Thinking	674
	Certification Questions	674

CHAPTER 12	Cloud Computing and Virtualization	676
	Chapter Outline	677
	Objectives	677
	Key Terms	677
12-1	Introduction	678

12-2	Virtualization	679
	Setting Up Virtualization on Windows 10	682
	Section 12-2 Review	691
	Test Your Knowledge	691
12-3	Cloud Computing	692
	Cloud Computing Service Models	694
	Cloud Infrastructures	696
	Section 12-3 Review	697
	Test Your Knowledge	698
12-4	Enterprise Storage	698
	Section 12-4 Review	700
	Test Your Knowledge	700
	Summary	701
	Questions and Problems	701
	Certification Questions	704

CHAPTER 13 **Codes and Standards** **706**

	Chapter Outline	707
	Objectives	707
	Key Terms	707
13-1	Introduction	708
13-2	Safety Standards and Codes	708
	Design and Construction Requirements for Exit Routes (29 CFR 1910.36)	709
	Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37)	710
	Emergency Action Plans (29 CFR 1910.38)	710
	Fire Prevention Plans (29 CFR 1910.39)	711
	Portable Fire Extinguishers (29 CFR 1910.157)	712
	Fixed Extinguishing Systems (29 CFR 1910.160)	713
	Fire Detection Systems (29 CFR 1910.164)	714
	Employee Alarm Systems (29 CFR 1910.165)	715
	Hazard Communication (29 CFR 1910.1200)	716
	HVAC Systems	717
	Door Access	717
	Section 13-2 Review	718
	Test Your Knowledge	718
13-3	Industry Regulatory Compliance	718
	FERPA	719
	FISMA	719
	GDPR	719

GLBA	719
HIPAA	720
PCI DSS	720
International Export Controls	720
Section 13-3 Review	722
Test Your Knowledge	722
13-4 Business Policies, Procedures, and Other Best Practices	723
Memorandum of Understanding	723
Service-Level Agreement	724
Master Service Agreement	724
Master License Agreement	724
Non-Disclosure Agreement	725
Statement of Work	725
Acceptable Use Policy	725
Incident Response Policy	725
Password Policy	726
Privileged User Agreement	726
Standard Operating Procedure	726
Onboarding and Offboarding Policies	727
Other Best Practices	727
Section 13-4 Review	728
Test Your Knowledge	728
13-5 Business Continuity and Disaster Recovery	729
Section 13-5 Review	732
Test Your Knowledge	732
Summary	733
Questions and Problems	733
Certification Questions	739

Glossary **742**

Index **764**

Online Only Elements:

- Net-Challenge Software
- Wireshark Captures
- Network+ quizzes

ABOUT THE AUTHORS

Jeffrey S. Beasley is a professor emeritus in the Information and Communications Technology program at New Mexico State University, where he taught computer networking and many related topics. He is coauthor of *Modern Electronic Communication*, ninth edition, the author of *Networking*, second edition, and co-author of *Networking Essentials*, fifth edition, and *A Practical Guide to Advanced Networking*.

Piyasat Nilkaew is the director of Computing and Networking Infrastructure at New Mexico State University and has more than 20 years of experience in network management and consulting. He has extensive expertise in deploying and integrating multiprotocol and multivendor data, voice, and video network solutions. He is co-author of *Networking Essentials*, fifth edition, and *A Practical Guide to Advanced Networking*.

ABOUT THE TECHNICAL REVIEWER

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

DEDICATIONS

This book is dedicated to my family: Kim, Damon/Heather, and Dana/Sam. —Jeff Beasley

This book is dedicated to my family: Boonsong, Pariya, June, Ariya, and Atisat. —Piyasat Nilkaew

ACKNOWLEDGMENTS

I am grateful to the many people who have helped with this text. My sincere thanks go to the following technical consultants:

- Danny Bosch and Matthew Peralta for sharing their expertise with optical networks and unshielded twisted-pair cabling
- Don Yates for his help with the initial Net-Challenge software

I would also like to thank my many past and present students for their help with this book:

- Abel Sanchez, Kathryn Sager, and Joshua Cook for their work on the Net-Challenge software; Adam Segura for his help taking pictures of the steps for CAT6 termination; Marc Montez, Carine George-Morris, Brian Morales, Michael Thomas, Jacob Ulibarri, Scott Leppelman, and Aarin Buskirk for their help with laboratory development; Josiah Jones and Raul Marquez Jr. for their help with the Wireshark material; and Ariya Nilkaew for her help with revising and editing many of the captured pictures

- Aaron Shapiro and Aaron Jackson for their help testing the many network connections presented in the text
- Paul Bueno and Anthony Bueno for reading through an early draft of the text

Your efforts are greatly appreciated.

We appreciate the excellent feedback of the following reviewers: Phillip Davis, DelMar College, Texas; Thomas D. Edwards, Carteret Community College, North Carolina; William Hessmiller, Editors & Training Associates; Bill Liu, DeVry University, California; and Timothy Staley, DeVry University, Texas.

Our thanks to the people at Pearson for making this project possible. Thanks to Brett Bartow for providing us with the opportunity to work on the sixth edition and for helping make this process enjoyable. Thanks to Marianne Bartow, to all the people at Pearson IT Certification, and also to the many technical editors for their help editing the manuscript.

Special thanks to our families for their continued support and patience.

—*Jeffrey S. Beasley and Piyasat Nilkaew*

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 authors and editors who worked on the book.

Email: community@informit.com

INTRODUCTION

This book provides a look at computer networking from the point of view of a network administrator. It guides readers from an entry-level knowledge of computer networks to advanced concepts related to Ethernet networks; router configuration; TCP/IP networks; routing protocols; local, campus, and wide area network configuration; network security; wireless networking; optical networks; voice over IP; network servers; and Linux networking. After reading the entire text, you will have gained a solid knowledge base in computer networks.

In our years of teaching, we have observed that technology students prefer to learn “how to swim” after they have gotten wet and taken in a little water. Then they are ready for more challenges. In this book, we therefore show you the technology, how it is used, and why, and you can take the applications of the technology to the next level. Allowing you to experiment with the technology helps you develop a greater understanding.

ORGANIZATION OF THE TEXT

This book has been thoroughly updated to reflect the latest version of the CompTIA Network+ exam. *Networking Essentials*, sixth edition, is a practical, up-to-date, and hands-on guide to the basics of networking. Written from the viewpoint of the network administrator, it requires absolutely no previous experience with either network concepts or day-to-day network management. Throughout the text, you will gain an appreciation of how basic computer networks and related hardware are interconnected to form a network. You will come to understand the concepts of twisted-pair cable, fiber optics, LANs interconnection, TCP/IP configuration, subnet masking, basic router configuration, switch configuration and management, wireless networking, and network security.

The textbook’s companion website contains laboratory exercises, the Net-Challenge software, Wireshark captures, and the Network+ terminology quizzes.

Key Pedagogical Features

- The *Chapter Outline*, *Network+ Objectives*, *Key Terms*, and *Introduction* at the beginning of each chapter clearly outline specific goals for you, the reader. Figure I-1 shows an example of these features.

Chapter Outline

Chapter Objectives

Introduction: Chapter opens clearly outline specific goals

Chapter Outline

4-1 Introduction
4-2 The IEEE 802.11 Wireless LAN Standard
4-3 802.11 Wireless Networking
4-4 Bluetooth, WiMAX, RFID, and Mobile Communications

Objectives

- Define the features of the 802.11 wireless LAN standard
- Understand the components of a wireless LAN
- Explore how wireless LANs are configured

Key Terms

WLAN	pseudorandom	paging procedure
basic service set (BSS)	hopping sequence	piconet
ad hoc network	OFDM	pairing
access point	OFDMA	passkey
transceiver	U-NII	WiMAX
extended service set (ESS)	MIMO	BWA
hand-off	MU-MIMO	NLOS
roaming	beamforming	last mile
CSMA/CA	Wi-Fi	radio frequency identification (RFID)
DSSS	SSID	backscatter
ISM band	site survey	Slotted Aloha
FHSS	inquiry procedure	

WLAN
Wireless local area network

This chapter examines the features and technologies used in a wireless local area network (WLAN). Wireless networking is an extension of computer networks to the radio frequency (RF) world. A WLAN provides increased flexibility and mobility for connecting to a network. A properly designed WLAN for a building provides mobile access for a user from virtually any location in the building. The user doesn't have to look for a connection to plug into; also, the expense of pulling cables and installing wall plates required for wired networks can be avoided. However, a network administrator must carefully plan a wireless LAN installation and have a good understanding of the issues of using WLAN technologies to ensure the installation of a reliable and secure network.

4-1 INTRODUCTION

The objective of this section is to introduce students to wireless networking. Wireless networks are being used everywhere, and it is a network administrator's job to ensure that the addition of a wireless network meets the connectivity, data throughput, and security requirements for the network.

This chapter addresses the basic issues of incorporating WLAN technologies into a network. Section 4-2, "The IEEE 802.11 Wireless LAN Standard," includes an overview of WLAN concepts and terminology, frequency allocations, and spread spectrum communication. The applications of WLANs are presented in Section 4-3, "802.11 Wireless Networking," which looks at various types of WLAN configurations, such as point-to-point and point-to-multipoint. Section 4-4, "Bluetooth, WiMAX, RFID, and Mobile Communications," looks at wireless networking technologies such as Bluetooth, WiMAX, and RFID. Any time a signal is transmitted over the air or even through a cable, there is some chance that the signal can be intercepted. Transmitting data over a wireless network introduces unique security issues. Section 4-5, "Configuring a Point-to-Multipoint Wireless LAN: A Case Study," presents an example of configuring a WLAN to provide access for users in a metropolitan area. Section 4-6 "Troubleshooting Wireless Networks" provides an overview of common techniques for troubleshooting wireless networks.

Table 4-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

Key Terms for this Chapter

FIGURE I-1

- The *Net-Challenge* software provides simulated hands-on experience configuring routers and switches. Exercises provided in the text (see Figure I-2) and companion website challenge you to undertake certain router/network configuration tasks. These challenges help you check your ability to enter basic networking commands and to set up router functions, such as configuring the interface (Ethernet and serial) and routing protocols (for example, RIP, static). The software has the look and feel of actually being connected to a router's console port.

Net-Challenge exercises are found throughout the text where applicable

Exercises challenge readers to undertake certain tasks

which is not saved in the router's nonvolatile random access memory (NVRAM). This means that when the router reboots, the configuration changes will be lost. To save the changes to the router's NVRAM to the startup configuration, use the **copy running-configuration startup-configuration** (or **copy run start** for short) command:

```
RouterA# copy run start
```

To verify the changes made and to view the running configuration, use the command **show running-configuration** (or **show run** for short). To view the saved configuration in NVRAM, use the command **show startup-configuration**:

```
RouterA# show run
RouterA# show startup-configuration
```

Router Configuration Challenge: Privileged EXEC Mode

For this challenge, you need to use the Net-Challenge software available from this book's companion website. Click the Net-ChallengeV5.exe file, and the program opens on your desktop (refer to Figure 7-6). The Net-Challenge software uses a three-router campus network scenario. You can view the topology for the network by clicking the **View Topology** button. Figure 7-11 shows the network topology used in the software. The software allows you to configure each of the three routers and to configure the network interface for computers in the LANs attached to each router. Clicking one of the router diagram symbols in the topology enables you to view the IP address for the router required for the configuration.

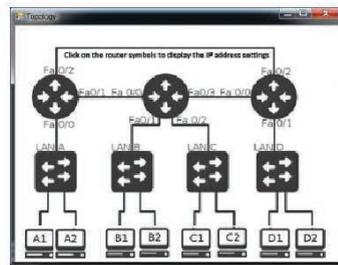


FIGURE 7-11 The network topology for Net-Challenge. The arrows indicate where to click to display the router IP address configurations.

You can connect to a router by clicking one of the three router buttons shown in Figure 7-4, earlier in this chapter. An arrow points to the buttons used to establish a console connection. Clicking a button connects the selected router to a terminal console session, enabling the simulated console terminal access to all three routers. The routers are marked with their default hostnames, Router A, Router B, and Router C.

This challenge tests your ability to use router commands in privileged EXEC mode, also called enable mode. In the Net-Challenge software, click the **Select Challenge** button to open a list of challenges available with the software. Select the **Privileged EXEC Mode** challenge to open the associated check box window. The tasks in each challenge will be checked as you complete them.

To begin the Privileged EXEC Mode challenge, follow these steps:

1. Make sure you are connected to Router A by clicking the appropriate selection button.
2. Demonstrate that you can enter the router's privileged EXEC mode. The router screen should display **Router#**. The password is **Chile**.
3. Place the router in terminal configuration mode [**Router(config)#**].
4. Use the **hostname** command to change the router's hostname to RouterA.
5. Set the enable secret for the router to **Chile**.
6. Set the vty password to **ConCarne**.
7. Configure the three FastEthernet interfaces on RouterA as follows:


```
FastEthernet0/0 (fa0/0) 10.10.20.250 255.255.255.0
FastEthernet0/1 (fa0/1) 10.10.200.1 255.255.255.0
FastEthernet0/2 (fa0/2) 10.10.100.1 255.255.255.0
```
8. Enable each of the router FastEthernet interfaces by using the **no shut** command.
9. Use the **sh ip interface brief** (or **sh ip int brief**) command to verify that the interfaces have been configured and are functioning. For this challenge, the interfaces on Router B and Router C have already been configured.
10. Configure the serial interfaces on the router. Serial0/0 is the DCE. Set the clock rate to 56000 and set the IP addresses and subnet masks as follows:


```
Serial 0/0 10.10.128.1 255.255.255.0
Serial 0/1 10.10.64.1 255.255.255.0
```
11. Use the **sh ip int brief** command to verify that the serial interfaces are properly configured. For this challenge, the interfaces on Router B and Router C have already been configured.
12. Use the **ping** command to verify that you have network connections for the following interfaces:


```
RouterA Fa0/1 (10.10.200.1) to RouterB Fa0/2 (10.10.200.2)
RouterA Fa0/2 (10.10.100.1) to RouterC Fa0/2 (10.10.100.2)
```

FIGURE I-2

- The textbook features and introduces how to use the *Wireshark network protocol analyzer*. Examples of using the software to analyze data traffic are included throughout the text. *Numerous worked-out examples* are included in every chapter to reinforce key concepts and aid in subject mastery, as shown in Figure I-3.

Examples using the Wireshark protocol analyzer are included throughout the text where applicable

Downloading and Installing Wireshark

To download and install the latest version of the Wireshark software, follow these steps:

1. Visit www.Wireshark.org, click **Download Wireshark**, and select your corresponding operating system.
2. Click **Run** when the dialog box appears to initiate the download process.
3. At the setup wizard prompt, select **Next** and agree to the license agreement.
4. Choose the components you would like to install and click **Next** to continue.
5. Select program shortcuts and click **Next** to continue.
6. Use the default directory paths specified in the setup menu and click **Install** to start the installation process.

When the Wireshark software is installed, you are ready to begin using it.

Using Wireshark to Capture Packets

In most cases, you will want to capture data packets from your own network. The following steps describe how to use Wireshark to capture packets:

1. In Windows, click **Start > Programs > Wireshark** and select **Wireshark** to start the program. In macOS, go to the **Applications** folder and then select **Wireshark** to start the program.
2. To capture packets on an operating network, select the interfaces in which you would like to obtain the capture (see Figure 10-23) by going to **Capture > Interfaces**. After selecting your interfaces, click **Start** to start capturing, as shown in Figure 10-24. You can also get to the interface list by clicking **Interface List** on the Wireshark home screen.
3. To examine the packets, stop the simulation by clicking **Capture > Stop**. Remember that there must be some activity on your network for packets to be transferred. You might see little traffic activity if your network is in the lab and there is limited network activity. You can always use the **ping** command to generate some network data activity, if needed.

To open a saved capture file, click **File > Open** or click **Open** on the Wireshark home screen.

To change capture options, click **Capture > Options** and change the options to your preferred settings.

10-8: NETWORK ANALYZER: WIRESHARK 561

FIGURE I-3

- *Key Terms* and their definitions are highlighted in the margins to foster inquisitiveness and ensure retention. Illustrations and photos are used throughout to aid in understanding the concepts discussed (see Figure I-4).

Key terms are highlighted in the text and defined in the margin

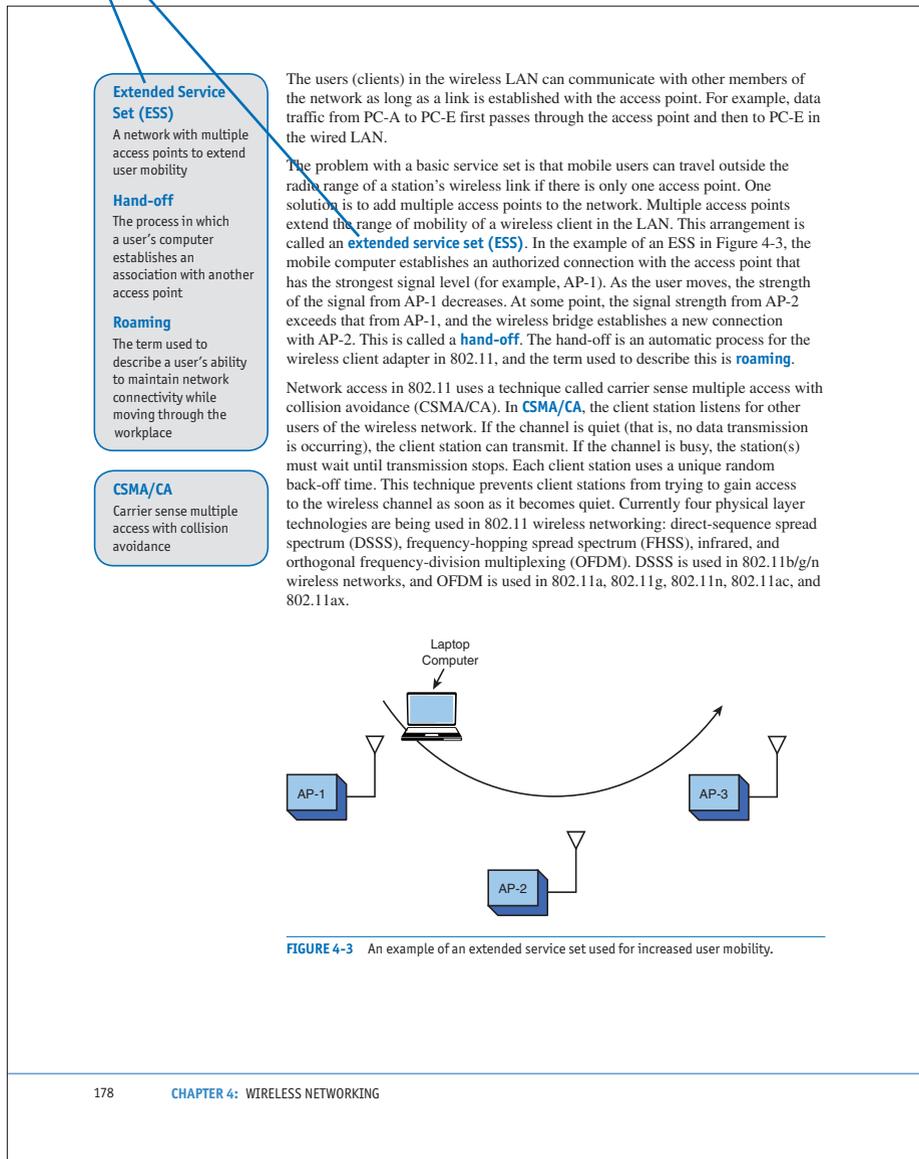


FIGURE I-4

- A *Summary*, *Questions and Problems*, *Critical Thinking*, and *Certification Questions* are provided at the end of each chapter, as shown in Figure I-5

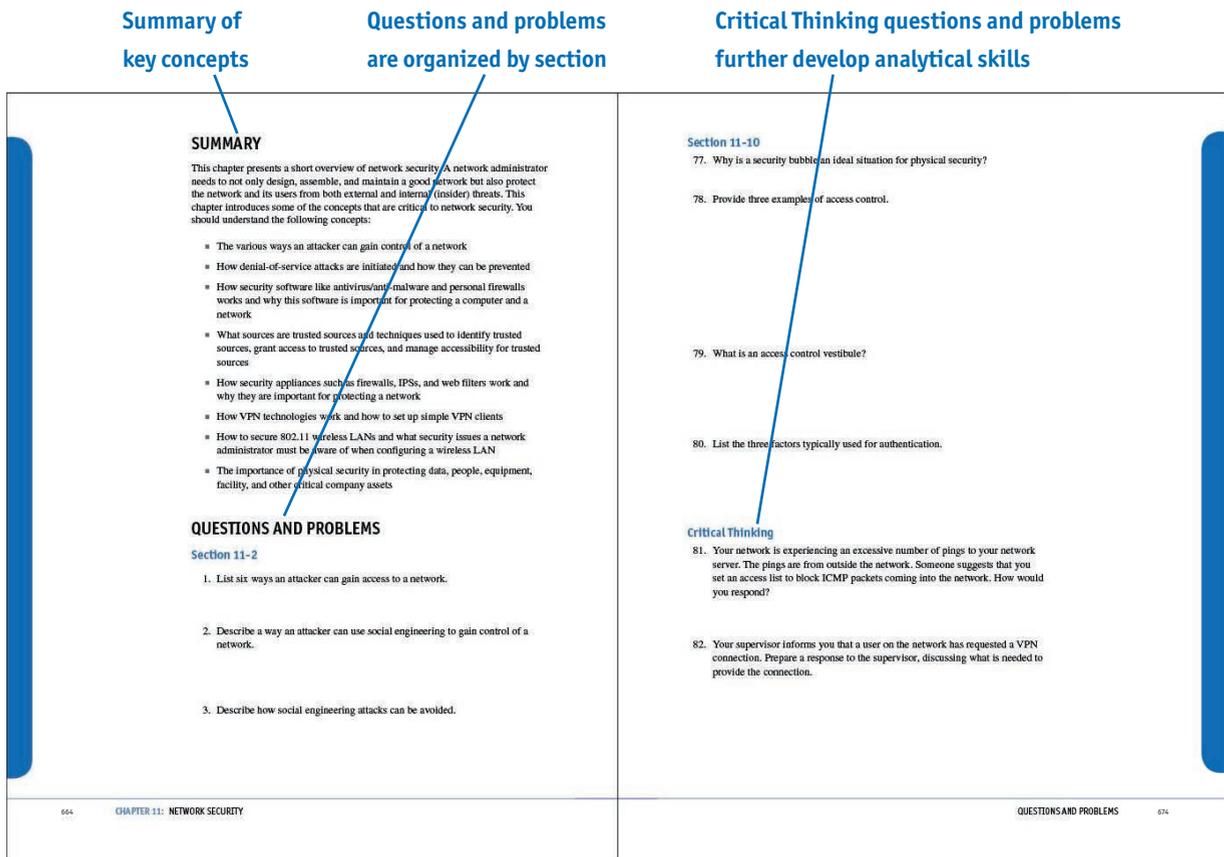


FIGURE I-5

- An extensive *Glossary* at the end of the book offers quick, accessible definitions to key terms and acronyms, and this book also includes an exhaustive *Index* (see Figure I-6).

Complete Glossary of terms and acronyms provide quick reference

Exhaustive Index provides quick reference

<p>? The help command, which can be used at any prompt in the command-line interface for the Cisco IOS software</p> <p>10GBASE-T Twisted-pair copper capable of 10Gbps</p> <p>3G/4G Third Generation and Fourth Generation, digital mobile phone technologies developed to provide broadband network wireless services</p> <p>6to4 prefix A globally routable address that enables IPv6 hosts to communicate over the IPv4 Internet</p> <p>802.1X An IEEE standard protocol for access control and authentication; also called dot1x</p> <p>8P8C The proper term for an RJ-45 modular plug</p> <p>A record (Address record) The most common record in DNS, which maps a hostname to an IP address</p> <p>AAAA record (Quad-A record) A DNS record for IPv6</p> <p>Absorption Light interaction with the atomic structure of the fiber material; also involves the conversion of optical power to heat</p> <p>Access control Physical security measures such as access control cards, possibly biometric access control systems, and lockable fencing</p> <p>Access control hardware Hardware used to identify and authenticate someone entering a facility</p> <p>Access control list (ACL) A basic form of firewall protection</p> <p>Access control vestibule/mantrap A control device that consists of two interlocking doors in which the first set of doors must be closed before the second set of doors can open</p> <p>access-list permit Ip any any The instruction added to the last line of an access list to allow all other data packets to enter and exit the router</p> <p>Access point A transceiver used to interconnect a wireless and a wired LAN</p> <p>ACK Acknowledgment packet, a packet in the TCP three-way connection handshake</p> <p>ACR A measurement that compares the signal level from a transmitter at the far end to the crosstalk measured at the near end</p> <p>Active/active An architecture in which both the primary site and the disaster recovery site are up and running at the same time</p> <p>Active/passive An architecture in which the disaster recovery site is idle, in standby mode</p> <p>Adaptive cut-through A mode that is a combination of the store-and-forward and cut-through modes</p> <p>Ad hoc network An independent network</p> <p>Address Resolution Protocol (ARP) A protocol used to map IP addresses to MAC addresses</p> <p>Administrative distance A feature used by routers to select the best path when more than one path is available</p> <p>Administratively down An indication that the router interface has been shut off by an administrator</p> <p>ADSL (Asymmetric DSL) A service that provides up to 1.544Mbps from the user to the service provider and up to 8Mbps back to the user from the service provider</p> <p>Advertise To share route information</p> <p>AES Advanced Encryption Standard, the encryption algorithm used by WPA2</p> <p>Aging time The length of time a MAC address remains assigned to a port</p> <p>AH Authentication Header, a security protocol that guarantees the authenticity of IP packets</p> <p>Alien crosstalk (AXT) Unwanted signal coupling from one permanent link to another</p> <p>Angled physical contact (APC) A green fiber connector whose endface is polished and has an 8-degree angle</p> <p>Ant+ An ultra-low-power wireless protocol for wireless sensor networks operating at 2.4GHz</p> <p>Anycast address An address obtained from a list of addresses</p> <p>APIPA Automatic Private IP Addressing, a Windows process that automatically configures reserved private IP addresses and subnet masks</p> <p>Application layer Layer 7 of the OSI model, which interacts with application programs that incorporate a communication component such as an Internet browser and email</p>	<p>Symbols</p> <p>? (help) command, 367</p> <p>Numbers</p> <p>3DES (Triple Data Encryption Standard), 651</p> <p>3G wireless standard, 204</p> <p>4G wireless standard, 204</p> <p>4G/LTE, 204</p> <p>5G wireless standard, 204</p> <p>6to4 prefix, 335</p> <p>8P8C connectors, 70-71</p> <p>10BASE2 cabling, 41</p> <p>10BASE3 cabling, 41</p> <p>10BASE-FL cabling, 41</p> <p>10BASE-T cabling, 41</p> <p>10GBASE-LR cabling, 41</p> <p>10GBASE-SR cabling, 41</p> <p>10GBASE-T cabling, 41, 76, 97-98</p> <p>AXT, 98</p> <p>full-duplex transmissions, 100</p> <p>F/UTP, 99</p> <p>hybrid echo cancellation circuits, 100</p> <p>IEEE 802.3an-2006, 98</p> <p>performance, 100-101</p> <p>PSAACRE, 98, 99</p> <p>PSANEXT, 98, 99</p> <p>signal transmission, 100-101</p> <p>29 CFR 1910.1200 (Hazard Communication), 716</p> <p>29 CFR 1910.157 (Portable Fire Extinguishers), 712-713</p> <p>29 CFR 1910.160 (Fixed Extinguishing Systems), 713-714</p> <p>29 CFR 1910.164 (Fire Detection Systems), 714-715</p> <p>29 CFR 1910.165 (Employee Alarm Systems), 715-716</p> <p>29 CFR 1910.36 (Design and Construction Requirements for Exit Routes), 709-710</p> <p>29 CFR 1910.37 (Maintenance, Safeguards, and Operational Features for Exit Routes), 710</p> <p>29 CFR 1910.38 (Emergency Action Plans), 710-711</p> <p>29 CFR 1910.39 (Fire Prevention Plans), 711-712</p> <p>32-bit CPU architectures, 679</p> <p>40GBASE-T cabling, 41</p> <p>64-bit CPU architectures, 679</p> <p>100BASE-FX cabling, 41</p> <p>100BASE-SX cabling, 41</p> <p>100BASE-TX cabling, 41</p> <p>802.1x (dot1x) wireless standard, 633</p> <p>802.11 wireless standard, 175-176</p> <p>ad hoc networks, 176, 177</p> <p>AP, 177-178</p> <p>BSS, 176, 177, 178</p> <p>channel bonding, 179</p> <p>CSMA/CD, 178</p> <p>DSSS, 179</p> <p>ESS, 178</p> <p>FHSS, 180</p> <p>frequency channels, 179</p> <p>hand-offs, 178</p> <p>hopping sequences, 180</p> <p>ISM band, 179</p> <p>MAC layer, 176</p> <p>OFDM, 180</p> <p>Open Authentication, 638</p> <p>PHY layer, 176</p> <p>pseudorandom numbering sequences, 180</p> <p>roaming, 178</p> <p>shared-key authentication, 638</p> <p>transceivers, 177</p> <p>transmit power, 180</p> <p>WMN, 176</p> <p>802.11a (Wi-Fi 2) wireless standard, 24, 180-181, 183</p> <p>802.11ac (Wi-Fi 5) wireless standard, 24, 182, 183</p> <p>802.11ax (Wi-Fi 6) wireless standard, 25, 182, 183</p> <p>802.11b (Wi-Fi 1) wireless standard, 24, 181, 183</p> <p>802.11g (Wi-Fi 3) wireless standard, 24, 181, 182, 183</p> <p>802.11i wireless standard, 183</p> <p>802.11n (Wi-Fi 4) wireless standard, 24, 181, 182, 183</p> <p>802.11r wireless standard, 183</p> <p>802.16a (WiMAX) wireless standard, 200</p> <p>1000BASE-LX cabling, 41</p> <p>1000BASE-SX cabling, 41</p>
GLOSSARY 743	INDEX 3

FIGURE I-6

Companion Website

The companion website includes the captured data packets used throughout the book. It also includes the Net-Challenge software, which was developed specifically for this text. The companion website also includes chapter-based quiz modules for you to test your knowledge and all of the key terms in an online flash card application. Finally, you can access your 10% off Network+ exam voucher from the companion website.

4

CHAPTER

Wireless Networking

Chapter Outline

4-1 Introduction
4-2 The IEEE 802.11 Wireless LAN Standard
4-3 802.11 Wireless Networking
4-4 Bluetooth, WiMAX, RFID, and Mobile Communications

4-5 Configuring a Point-to-Multipoint Wireless LAN: A Case Study
4-6 Troubleshooting Wireless Networks
Summary
Questions and Problems

Objectives

- Define the features of the 802.11 wireless LAN standard
- Understand the components of a wireless LAN
- Explore how wireless LANs are configured
- Examine how site surveys are done for wireless LANs
- Investigate the issues of securing a wireless LAN
- Explore how to configure a point-to-multipoint wireless LAN

Key Terms

WLAN	pseudorandom	paging procedure
basic service set (BSS)	hopping sequence	piconet
ad hoc network	OFDM	pairing
access point	OFDMA	passkey
transceiver	U-NII	WiMAX
extended service set (ESS)	MIMO	BWA
hand-off	MU-MIMO	NLOS
roaming	beamforming	last mile
CSMA/CA	Wi-Fi	radio frequency
DSSS	SSID	identification (RFID)
ISM band	site survey	backscatter
FHSS	inquiry procedure	Slotted Aloha

WLAN

Wireless local area network

This chapter examines the features and technologies used in a wireless local area network (**WLAN**). Wireless networking is an extension of computer networks into the radio frequency (RF) world. A WLAN provides increased flexibility and mobility for connecting to a network. A properly designed WLAN for a building provides mobile access for a user from virtually any location in the building. The user doesn't have to look for a connection to plug into; also, the expense of pulling cables and installing wall plates required for wired networks can be avoided. However, a network administrator must carefully plan a wireless LAN installation and have a good understanding of the issues of using WLAN technologies to ensure the installation of a reliable and secure network.

4-1 INTRODUCTION

The objective of this section is to introduce students to wireless networking. Wireless networks are being used everywhere, and it is a network administrator's job to ensure that the addition of a wireless network meets the connectivity, data throughput, and security requirements for the network.

This chapter addresses the basic issues of incorporating WLAN technologies into a network. Section 4-2, "The IEEE 802.11 Wireless LAN Standard," includes an overview of WLAN concepts and terminology, frequency allocations, and spread spectrum communication. The applications of WLANs are presented in Section 4-3, "802.11 Wireless Networking," which looks at various types of WLAN configurations, such as point-to-point and point-to-multipoint. Section 4-4, "Bluetooth, WiMAX, RFID, and Mobile Communications," looks at wireless networking technologies such as Bluetooth, WiMAX, and RFID. Any time a signal is transmitted over the air or even through a cable, there is some chance that the signal can be intercepted. Transmitting data over a wireless network introduces unique security issues. Section 4-5, "Configuring a Point-to-Multipoint Wireless LAN: A Case Study," presents an example of configuring a WLAN to provide access for users in a metropolitan area. Section 4-6 "Troubleshooting Wireless Networks" provides an overview of common techniques for troubleshooting wireless networks.

Table 4-1 outlines the CompTIA Network+ objectives related to this chapter and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments on the Network+ objectives presented in that section. These comments are provided to help reinforce your understanding of each Network+ objective. The chapter review also includes "Test Your Knowledge" questions to help you understand key concepts before you advance to the next section of the chapter. At the end of the chapter you will find a complete set of questions as well as sample certification exam-type questions.

TABLE 4-1 Chapter 4 CompTIA Network+ Objectives

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	Networking Fundamentals	
1.2	Explain the characteristics of network topologies and network types.	4-2
1.3	Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	4-4
1.6	Explain the use and purpose of network services.	4-2, 4-3
1.7	Explain basic corporate and datacenter network architecture.	4-4
2.0	Network Implementations	
2.1	Compare and contrast various devices, their features, and their appropriate placement on the network.	4-2, 4-3, 4-4, 4-5
2.3	Given a scenario, configure and deploy common Ethernet switching features.	4-2, 4-4
2.4	Given a scenario, install and configure the appropriate wireless standards and technologies.	4-2, 4-3, 4-4, 4-5
3.0	Network Operations	
3.1	Given a scenario, use the appropriate statistics and sensors to ensure network availability.	4-2, 4-3, 4-4
3.2	Explain the purpose of organizational documents and policies.	4-3, 4-5
3.3	Explain high availability and disaster recovery concepts and summarize which is the best solution.	4-2, 4-5
4.0	Network Security	
4.3	Given a scenario, apply network hardening techniques.	4-2, 4-4, 4-5
4.4	Compare and contrast remote access methods and security implications.	4-2
5.0	Network Troubleshooting	
5.2	Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	4-2, 4-3, 4-4
5.4	Given a scenario, troubleshoot common wireless connectivity issues.	4-2, 4-3, 4-5, 4-6
5.5	Given a scenario, troubleshoot general networking issues.	4-4

4-2 THE IEEE 802.11 WIRELESS LAN STANDARD

The anatomy of 802.11 wireless networking is presented in this section. This section introduces the basic service set wireless network, the extended service set, the independent basic service set (ad hoc), the frequencies used for wireless networks, the power output, and spread spectrum communications. Many topics are presented, including the 802.11 wireless (Wi-Fi) standards. Students need to be aware of these topics to fully comprehend how a wireless network functions.

A typical computer network uses twisted-pair and fiber-optic cable to interconnect LANs. Another media option competing for use in higher-data-rate LANs is

wireless, based on the IEEE 802.11 wireless standard. The advantages of wireless include the following:

- It is cost-effective for use in areas that are difficult or too costly to wire.
- It enables user mobility in the workplace.

Wireless networks have become the network of choice in environments such as homes, small offices, and public places. Being able to connect to a network without a wire is convenient for users, and the cost is relatively low. In the age of laptops and mobile devices, wireless opens the door to user mobility in the workplace, and user mobility provides flexibility. Workers can potentially access the network or wireless data services from virtually any location within the workplace. Accessing information from the network is as easy as if the information were on a USB drive.

The benefits of wireless networks in the workplace are numerous. To provide wireless connectivity, a network administrator must be sure the network services are reliable and secure. In order to provide reliable network services, an administrator must have a good understanding of WLAN configurations and technologies. This and the following sections examine the fundamentals of wireless networking, the 802.11 standard and its family (802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax), and how WLANs are configured.

The IEEE 802.11 WLAN standard defines the physical (PHY) layer, the media access control (MAC) layer, and the MAC management protocols and services.

The PHY layer defines the following:

- The method of transmitting the data, which can be either RF or infrared (although infrared is rarely used)
- How it interfaces with the MAC layer
- The reliability of the data service
- Access control to the shared wireless medium
- Privacy protection for transmitted data

The wireless management protocols and services are authentication, association, data delivery, and privacy.

The fundamental topology of a WLAN is the **basic service set (BSS)**. This is also called the independent basic service set, or **ad hoc network**. Figure 4-1 provides an example of an ad hoc network. In this network, the wireless clients (stations) communicate directly with each other. This means the clients have recognized the other stations in the WLAN and have established a wireless data link.

A related concept is a wireless mesh network (WMN), which is a communications network made up of Wi-Fi radios connected in a mesh topology (that is, a heavily interconnected network). A WMN is basically a wireless ad hoc network.

Basic Service Set (BSS)

An independent network

Ad hoc network

An independent network

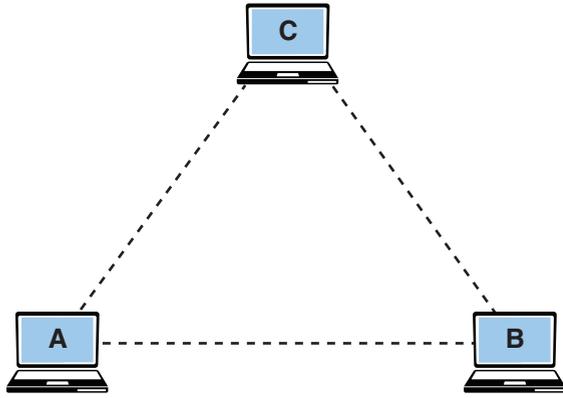


FIGURE 4-1 An example of an independent basic service set, or ad hoc, network.

The performance of the basic service set can be improved by including an **access point**, which is a transmit/receive unit (**transceiver**) that interconnects data from the wireless LAN to the wired network. In addition, the access point provides 802.11 MAC layer functions and supports bridge protocols. The access point typically uses an RJ-45 jack for connecting to the wired network. If an access point is being used, users establish a wireless communications link through it to communicate with other users in the WLAN or the wired network, as shown in Figure 4-2.

Access Point

A transceiver used to interconnect a wireless LAN and a wired LAN

Transceiver

A transmit/receive unit

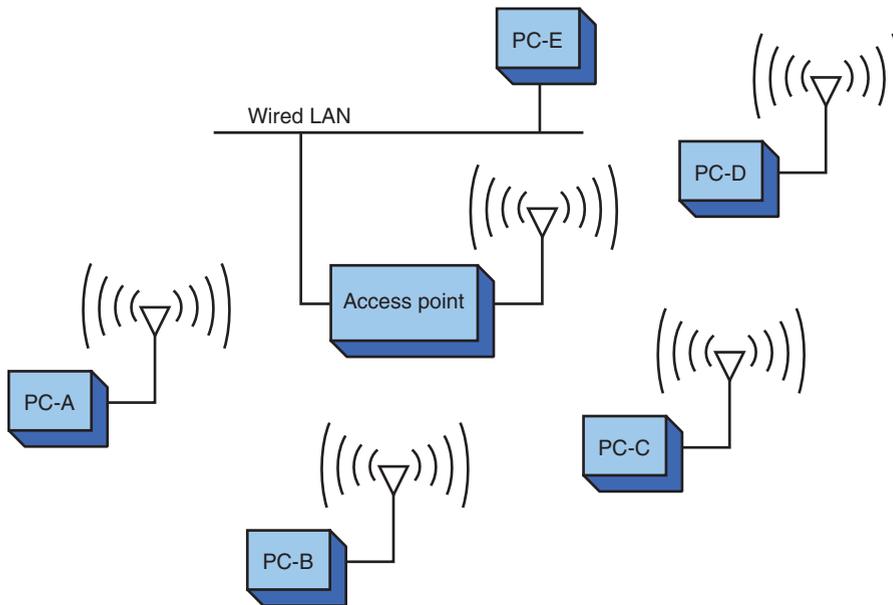


FIGURE 4-2 Adding an access point to a basic service set.

If data is being sent from PC-A to PC-D in the network shown in Figure 4-2, the data is first sent to the access point and then relayed to PC-D. Data sent from a wireless client to a client in the wired LAN also passes through the access point.

Extended Service Set (ESS)

A network with multiple access points to extend user mobility

Hand-off

The process in which a user's computer establishes an association with another access point

Roaming

The term used to describe a user's ability to maintain network connectivity while moving through the workplace

CSMA/CA

Carrier sense multiple access with collision avoidance

The users (clients) in the wireless LAN can communicate with other members of the network as long as a link is established with the access point. For example, data traffic from PC-A to PC-E first passes through the access point and then to PC-E in the wired LAN.

The problem with a basic service set is that mobile users can travel outside the radio range of a station's wireless link if there is only one access point. One solution is to add multiple access points to the network. Multiple access points extend the range of mobility of a wireless client in the LAN. This arrangement is called an **extended service set (ESS)**. In the example of an ESS in Figure 4-3, the mobile computer establishes an authorized connection with the access point that has the strongest signal level (for example, AP-1). As the user moves, the strength of the signal from AP-1 decreases. At some point, the signal strength from AP-2 exceeds that from AP-1, and the wireless bridge establishes a new connection with AP-2. This is called a **hand-off**. The hand-off is an automatic process for the wireless client adapter in 802.11, and the term used to describe this is **roaming**.

Network access in 802.11 uses a technique called carrier sense multiple access with collision avoidance (CSMA/CA). In **CSMA/CA**, the client station listens for other users of the wireless network. If the channel is quiet (that is, no data transmission is occurring), the client station can transmit. If the channel is busy, the station(s) must wait until transmission stops. Each client station uses a unique random back-off time. This technique prevents client stations from trying to gain access to the wireless channel as soon as it becomes quiet. Currently four physical layer technologies are being used in 802.11 wireless networking: direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), infrared, and orthogonal frequency-division multiplexing (OFDM). DSSS is used in 802.11b/g/n wireless networks, and OFDM is used in 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax.

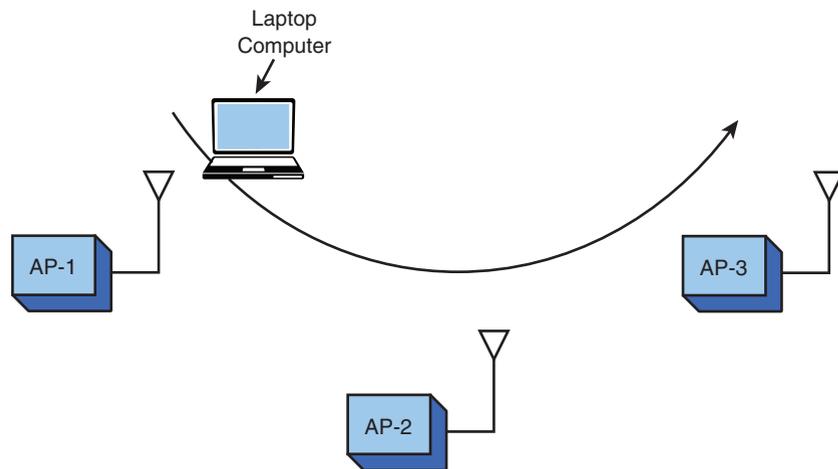


FIGURE 4-3 An example of an extended service set used for increased user mobility.

802.11 **DSSS** implements 14 channels (each consuming 22MHz) over approximately 90MHz of RF spectrum in the 2.4GHz **ISM** (industrial, scientific, and medical) **band**. DSSS is a technique used to spread the transmitted data over a wide bandwidth; in this case, it is a 22MHz bandwidth channel. A channel is a medium through which information is transmitted between transmitter and receiver. The bandwidth is a measure of the upper to lower frequencies of the channel required to transmit the information.

DSSS

Direct-sequence spread spectrum

ISM band

Industrial, scientific, and medical band

A related concept is *channel bonding*, in which two adjacent channels are combined to facilitate an increase in throughput between wireless devices. This is also called *Ethernet bonding* and is used in Wi-Fi applications.

Table 4-2 lists the frequency channels used in North America. Note that only 11 out of 14 channels are made available in North America due to regulatory requirements of the Federal Communication Commission (FCC). Figure 4-4 shows an example of the frequency spectrum for three-channel DSSS. Note that the three channels listed in Figure 4-4 (1, 6, and 11) do not overlap, while Table 4-2 shows that the other channels do have channel overlap. Remember that each channel is 22MHz in bandwidth. For example, channel 2 extends from 2.406GHz to 2.429GHz, with a center frequency of 2.417GHz, which clearly overlaps a portion of channel 1 and channel 3. Channels 1, 6, and 11 are the only channels that do not have overlap.

TABLE 4-2 North American DSSS Channels

Channel Number	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

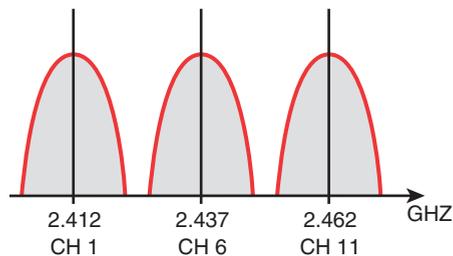


FIGURE 4-4 An example of the three channels in the DSSS spectrum.

FHSS

Frequency-hopping spread spectrum, a technique in which the transmit signal frequency changes based on a pseudorandom sequence

Pseudorandom

A number sequence that appears random but actually repeats

Hopping Sequence

The order of frequency changes

In frequency-hopping spread spectrum (**FHSS**), the transmit signal frequency changes based on a pseudorandom sequence. **Pseudorandom** means the sequence appears to be random but in fact does repeat, typically after some lengthy period of time. FHSS uses 79 channels (each 1MHz wide) in the ISM 2.4GHz band. FHSS requires that the transmitting and receiving units know the **hopping sequence** (the order of frequency changes) so that a communication link can be established and synchronized. FHSS data rates are typically 1Mbps and 2Mbps. FHSS is not commonly used anymore for wireless LANs. It's still part of the standard, but very few (if any) FHSS wireless LAN products are sold.

The maximum transmit power of 802.11b wireless devices is 1000 mW; however, the nominal transmit power level is 100 mW. The 2.4GHz frequency range used by 802.11b/g is shared by many technologies, including Bluetooth, cordless telephones, and microwave ovens.

LANs emit significant RF noise in the 2.4GHz range that can affect wireless data. A significant improvement in wireless performance is available with the IEEE 802.11a standards. The 802.11a equipment operates in the 5GHz range and provides significant improvement over 802.11b with respect to RF interference. An important concept related to noise is signal-to-noise ratio, which is a measure of the signal level relative to the noise level. The value is usually expressed in decibels (dB), and a high dB value is desirable.

Another technique used in the 802.11 standard is **orthogonal frequency-division multiplexing (OFDM)**. The basic idea with this technique is to divide the signal bandwidth into smaller subchannels and to transmit the data over these subchannels in parallel. These subchannels can be overlapping, but they do not interfere with each other. The subchannels are mathematically orthogonal, and this setup yields uncorrelated or independent signals.

The 802.11a standard transports data over 12 possible channels in the Unlicensed National Information Infrastructure (**U-NII**). The FCC set aside U-NII to support short-range, high-speed wireless data communications. The 802.11 channels and frequencies are governed by FCC regulations, which are periodically revised. A wireless manufacturer must keep its products up to date due to the regulatory impacts. Table 4-3 lists the operating frequencies for 802.11a, and Table 4-4 lists the transmit power levels for 802.11a.

OFDM

Orthogonal frequency-division multiplexing, a technique that involves dividing the signal bandwidth into smaller subchannels and transmitting the data over these subchannels in parallel

U-NII

Unlicensed National Information Infrastructure

TABLE 4-3 IEEE 802.11a Channels and Operating Frequencies

Channel	Center Frequency (GHz)	
36	5.180	
40	5.20	Lower band
44	5.22	
48	5.24	
52	5.26	
56	5.28	Middle band
60	5.30	
64	5.32	

Channel	Center Frequency (GHz)	
149	5.745	
153	5.765	Upper band
157	5.785	
161	5.805	

TABLE 4-4 Maximum Transmit Power Levels for 802.11a with a 6 dBi Antenna Gain

Band	Power Level
Lower	40 mW
Middle	200 mW
Upper	800 mW

IEEE 802.11a equipment is not compatible with 802.11b or 802.11g. The upside of this is that 802.11a equipment does not interfere with 802.11b or g; therefore, 802.11a and 802.11b/g links can run next to each other without causing interference. 802.11n can operate either in the 2.4GHz range or the 5GHz range. Cheaper 802.11n wireless cards tend to be manufactured with only 2.4GHz antennas, so users have to check the frequency specifications as not all 802.11n equipment has both 2.4GHz and 5GHz frequencies. Figure 4-5 shows an example of the two links operating together. Along the same lines, frequency mismatch is an issue if the two ends of the communications link are operating on different channels or if you are trying to make 802.11a communicate with 802.11b, as the frequencies are not compatible.

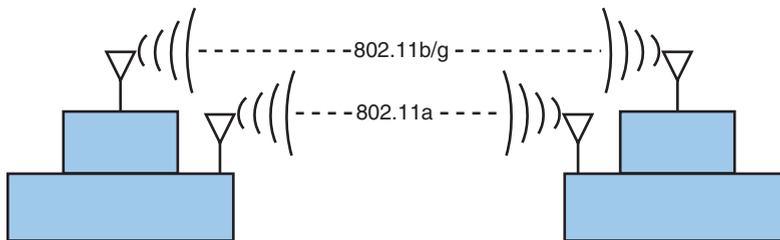


FIGURE 4-5 An example of an 802.11a installation and an 802.11b link running alongside each other.

The downsides of 802.11a are the increased cost of the equipment and increased power consumption because of the OFDM technology. This is of particular concern with mobile users because of the effect it can have on battery life. However, the maximum usable distance (RF range) for 802.11a is about the same as or even greater than that of 802.11b/g/n/ac/ax. It is important to note that any RF signal has distance limitations either due to limited output transmitted power, antenna pattern, or terrain issues.

Another IEEE 802.11 wireless standard is IEEE 802.11g. The 802.11g standard supports the higher data transmission rates of 54Mbps but operates in the same 2.4GHz range as 802.11b. The 802.11g equipment is also backward compatible with 802.11b equipment. This means that 802.11b wireless clients can communicate with the 802.11g access points, and the 802.11g wireless client equipment can communicate with the 802.11b access points. The obvious advantage of this is that a company with an existing 802.11b wireless network can migrate to the higher data rates provided by 802.11g without having to sacrifice network compatibility. In fact, new wireless equipment supports both the 2.4GHz and 5GHz standards, and it therefore has the flexibility of high speed, compatibility, and noninterference.

Another entry into wireless networks is 802.11n. This wireless technology operates in the same ISM frequency as 802.11b/g (2.4GHz) and can also operate in the 5GHz band. A significant improvement with 802.11n is multiple-input multiple-output (**MIMO**). MIMO uses a technique called space-division multiplexing, in which the data stream is split into multiple parts called spatial streams. The different spatial streams are transmitted using separate antennas. With MIMO, doubling the spatial streams doubles the effective data rate. The downside of this is the possibility of increased power consumption. The 802.11n specification includes a MIMO power-save mode. With this mode, 802.11n uses multiple data paths only when faster data transmission is required—thus saving power.

The 802.11ac technology operates in the 5GHz band. It uses a newer version of MIMO technology with eight spatial streams and has channels up to 80MHz wide. It also introduces multiuser MIMO (**MU-MIMO**), which can send MIMO spatial streams to multiple clients at the same time. 802.11ac incorporates standardized **beamforming**, a technique that is used to direct transmission of the radio signal to a specific device. Beamforming increases data throughput and reduces power consumption. 802.11n used beamforming, but it was not standardized. The transmit range for 802.11ac is similar to or better than that of 802.11n.

The latest addition to the 802.11 family is 802.11ax, also known as Wi-Fi 6. Whereas 802.11ac operates in the 5GHz band only, 802.11ax operates in both 2.4GHz and 5GHz bands. 802.11ax uses OFDMA (orthogonal frequency-division multiple access) rather than OFDM. OFDMA allows multiple users or clients to share the same channel simultaneously. Wireless devices can optionally support WPA3 (Wi-Fi Protected Access 3), but 802.11ax increases security requirements by mandating the use of WPA3 as its encryption and authentication standard. WPA3 is discussed in more detail in Chapter 11, “Network Security.”

Table 4-5 provides a comparison of 802.11n, 802.11ac, and 802.11ax in terms of their compatibility with other Wi-Fi technologies and the frequencies supported.

TABLE 4-5 **A Comparison of 802.11ac, 802.11n, and 802.11ax**

	802.11n	802.11ac	802.11ax
Backward-compatible with	802.11g, 802.11b, and 802.11a	802.11n	802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac
Frequencies supported	2.4GHz and 5GHz	5GHz	2.4GHz and 5GHz

MIMO

Multiple-input multiple-output

MU-MIMO

Multiuser Multiple-input Multiple-output

Beamforming

A technique used to direct transmission of a radio signal to a specific device

Wireless networks also go by the name **Wi-Fi**, which is not an acronym, but a term created and is a trademark of Wi-Fi Alliance to represent the standards for wireless communication. Wi-Fi is sometimes referred to as *wireless fidelity*. The Wi-Fi Alliance is an organization whose function is to test and certify wireless equipment for compliance with the 802.11x standards, the group of wireless standards developed under the IEEE 802.11 standard. The following list provides a summary of the most common wireless standards:

Wi-Fi

A term created and is a trademark of the Wi-Fi Alliance to represent the standards for wireless communication.

- **802.11b (Wi-Fi 1):** This standard can provide data transfer rates up to 11Mbps with ranges of 100–150 feet. It operates at 2.4GHz and uses DSSS.
- **802.11a (Wi-Fi 2):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 75 feet. It operates at 5GHz and uses OFDM.
- **802.11g (Wi-Fi 3):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 150 feet. It operates at 2.4GHz and uses DSSS or OFDM.
- **802.11n (Wi-Fi 4):** This high-speed wireless connectivity promises data transfer rates over 200Mbps. It operates at 2.4GHz and 5GHz and uses DSSS or OFDM.
- **802.11i:** This standard for WLANs provides improved data encryption for networks that use the 802.11a, 802.11b, and 802.11g standards.
- **802.11r:** This standard is designed to speed hand-offs between access points or cells in a WLAN. This standard is a critical addition to 802.11 WLANs if voice traffic is to become widely deployed.
- **802.11ac (Wi-Fi 5):** This is currently the most deployed wireless standard. It provides single-station data transfer rates of 500Mbps up to 1.3Gbps and operates in the 5GHz frequency band.
- **802.11ax (Wi-Fi 6):** This is the latest wireless standard, and manufacturers are starting to ship more equipment with this wireless technology. Theoretically, it could deliver close to 10Gbps data rates.

Another wireless technology is Z-Wave. This wireless communications protocol was developed for home automation. Typical applications include sensors for home lighting, security systems, and HVAC systems. The operating frequencies for Z-Wave in the United States are 908.4MHz and 916MHz.

Another entry into the ultra-low-power wireless protocol space is ANT+, which is used for wireless sensor networks (WSNs). This technology operates at 2.4GHz.

Section 4-2 Review

This section covers the following Network+ exam objectives.

1.2 Explain the characteristics of network topologies and network types.
This section introduces the new wireless technologies Z-Wave and ANT+.

1.6 Explain the use and purpose of network services.
This section provides an example of a network in which the wireless clients (stations) communicate directly with each other.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
An access point is a transmit/receive unit (transceiver) that interconnects data from the wireless LAN to the wired network. In addition, an access point provides 802.11 MAC layer functions and supports bridge protocols.

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.
This section introduces the terms basic service set, extended service set, and ad hoc set and the concept of roaming.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
This section examines the 802.11a/b/g/n/i/r/ac/ax standards as well as issues such as transmit distance, data speed, and frequencies. This section also introduces the concept of MIMO, which is used to increase the effective transmit data rate.

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.
To provide reliable network services, an administrator must have a good understanding of WLAN configurations and technologies.

4.3 Given a scenario, apply network hardening techniques.
Table 4-3 lists the operating frequencies for 802.11a, and Table 4-4 lists the transmit power levels for 802.11a.

4.4 Compare and contrast remote access methods and security implications.
This section introduces wireless management protocols and indicates that the services are authentication, association, data delivery, and privacy.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.
Technical issues related to throughput, speed, and distance are examined in this section.

Test Your Knowledge

1. True or false: 802.11ac networking equipment is compatible with 802.11b.

True

2. True or false: 802.11g networking equipment is compatible with 802.11b.

True

3. True or false: 802.11a and 802.11b wireless networks can run side-by-side.

True

4. True or false: 802.11ac networking equipment is compatible with 802.11n.

True

4-3 802.11 WIRELESS NETWORKING

This section introduces techniques for assembling a wireless network and helps students understand the purpose of the access point and the SSID (service set identifier). The techniques for implementing point-to-point and point-to-multipoint wireless networks are presented, and so is the very important concept of a site survey. Make sure students understand the importance of performing a good site survey to ensure user mobility and connectivity.

A wireless LAN can be configured in many ways to meet the needs of an organization. Figure 4-6 provides an example of a basic 802.11b/g/n/ac/ax WLAN configuration. In this configuration, each PC is outfitted with a wireless LAN adapter card. Today, most computer desktops and especially computer laptops are equipped with wireless adapters. For devices that lack these cards, an external USB wireless adapter can be used. A wireless adapter (or wireless LAN adapter) is a device that connects a client to the wireless medium, which is typically a radio wave channel in the 2.4GHz or 5GHz ISM band. The wireless medium can also be infrared, although that is not used very often. The following services are provided by a wireless LAN adapter:

- Delivery of the data
- Authentication
- Privacy

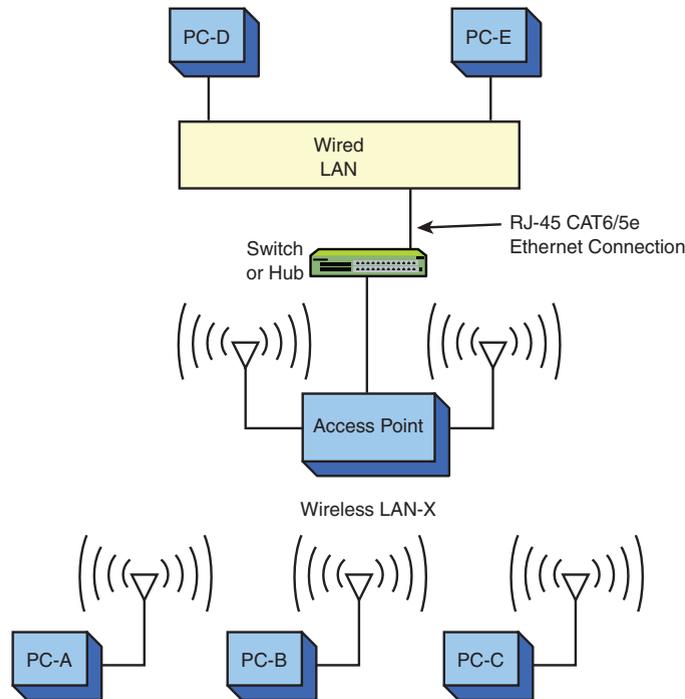


FIGURE 4-6 The setup for a basic WLAN.

One of the biggest misconceptions about wireless is that it does not require a wired connection. This is not quite correct. The connection to a wired LAN is provided by a wireless access point (WAP), which provides a bridge between the wireless LAN and the wired network. A physical cable connection (typically CAT6 or higher) ties the access point to the wired network's switch or hub (typically Ethernet).

For example, computer PC-A in Figure 4-6 sends a data packet to PC-D, a destination in the wired LAN. PC-A first sends a data packet over the wireless link. The access point recognizes the sender of the data packet as a host in wireless LAN-X and allows the wireless data to enter the access point. At this time, the data is sent out the physical Ethernet connection to the wired LAN. The data packet is then delivered to PC-D in the wired LAN.

How does the access point know that the wireless data packet is being sent from a client in the wireless LAN? The 802.11 wireless LAN devices use an **SSID** to identify what wireless data traffic is allowed to connect to the network. The SSID is the wireless *service set identifier*, which enables the client to join the wireless network.

The access point uses the SSID to determine whether the client is to become a member of the wireless network. The term *association* is used to describe a wireless connection that is made. The wrong SSID prevents an association, keeping the client from being able to become a member of the wireless network.

People are commonly surprised by the fact that an access point has two antennas. The two antennas implement *spatial diversity*, improving received signal gain and performance.

SSID

Service set identifier, a password that enables the client to join the wireless network

Figure 4-7 provides an example of the information displayed on the wireless adapter's console port when an association is made. The text indicates that a connection has been made to a parent (access point) whose MAC address is 00-40-96-25-9d-14. The text indicates that this MAC address has been added to the list of associations. This type of information is typically available via the wireless management software that comes with the wireless PC or PCMCIA adapter.

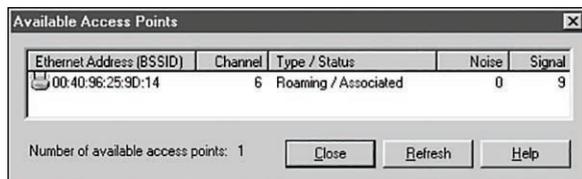


FIGURE 4-7 An example of the information displayed when an association is formed between a client and an access point.

An access point uses an association to build a table of users (clients) on the wireless network; this association table lists the MAC addresses for each networking device connected to the wireless network. Figure 4-8 provides an example of an association table. The access point uses the association table to forward data packets between the access point and the wireless network. As shown in Figure 4-8, the wireless client adapter also notifies the user if the client has lost an association with the access point.

A wireless bridge is a popular choice for connecting LANs that are running similar network protocols, even if the LANs are miles apart. Figure 4-9 provides examples. Figure 4-9(a) shows a point-to-point wireless bridge. Each building shown in Figure 4-9(a) has a connection from the wireless bridge to the building's LAN, as shown in Figure 4-10. The wireless bridge then connects to an antenna placed on the roof. A clear (line-of-sight) transmission path must exist between the two buildings; otherwise, signal *attenuation* (loss) or signal disruption can result. Antenna selection is also critical when configuring the connection. (This issue is addressed in Section 4-5.) The antenna must be selected so that the signal strength at the receiving site is sufficient to meet the required received signal level.



FIGURE 4-8 An example of a lost association.

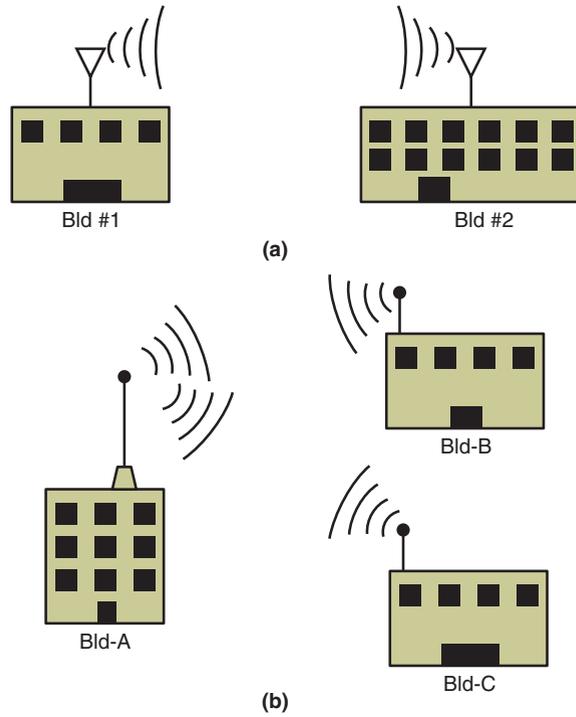


FIGURE 4-9 Examples of (a) point-to-point and (b) point-to-multipoint wireless bridge configurations.

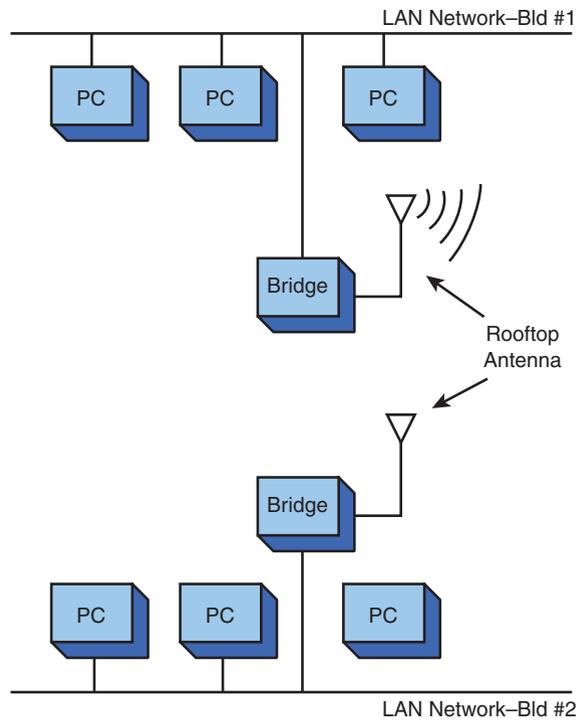


FIGURE 4-10 The wireless bridge connection to the wired network inside the building.

Figure 4-9(b) shows how a wireless bridge can be used to connect multiple remote sites to the main transmitting facility. Each building uses a bridge setup similar to that shown in Figure 4-10. The bridge connects to its respective LAN. In this case, Bld-A uses an antenna that has a wide coverage area (radiation pattern). The key objective with antenna selection is that the antenna must provide coverage for all receiving sites (in this case, Bld-B and Bld-C).

Wireless controllers are commonly used in enterprise wireless environments when managing hundreds of APs or more. In a traditional stand-alone wireless environment, each AP is managed individually. In an enterprise wireless controller environment, an AP communicates with its controller when booting up to download its necessary firmware and software, to register and authenticate itself, to receive its network information settings, and to receive its wireless LAN (WLAN) configuration. The wireless controller becomes the brain and manager of the whole operation. When wireless changes need to be made, they can be made at the controller, which pushes the changes out to all of the APs. CAPWAP (Configuration and Provisioning of Wireless Access Points) is the underlying wireless control protocol that APs use to communicate with wireless controllers. It supersedes LWAPP (Lightweight Access Point Protocol), which is a Cisco-proprietary protocol.

Wireless capacity is an issue today with the ever-increasing number of wireless users. Device density is the number of connecting wireless clients, and it has to be considered. Every wireless access point has a maximum device density that it can handle at one time. From a system design perspective, you have to plan for potential overcapacity with high-density Wi-Fi hotspots that can accommodate video streaming, image downloads, and multiple clients. Make sure you select access points that can handle the bandwidth demand; you don't want your clients to have to sacrifice bandwidth, especially when a cell phone can be set up as a hotspot that a wireless device can use to connect to the Internet via the data plan.

With wireless LANs, there is a maximum distance the signal can be transmitted. The distance limitation is a critical issue inside buildings when user mobility is required. Many obstacles can reflect and attenuate signals, causing reception to suffer. Also, the signal level for mobile users is hampered by increased distance from the access point. Distance is also a critical issue in outdoor point-to-multipoint wireless networks.

A solution is to place multiple wireless access points within the facility, as shown in Figure 4-11. Mobile clients can maintain a connection as they travel through the workplace because the wireless client automatically selects the access point that provides the strongest signal level. The access points can be arranged so that overlapping coverage of the workplace is provided, thus enabling seamless roaming for the client. The signal coverage is shown as circles in Figure 4-11. In actual practice, the radiation patterns are highly irregular due to reflections of the transmitted signal.

To have good wireless coverage in a large environment, it is not unusual to see the number of wireless access points in the range of hundreds or thousands. When dealing with so many wireless access points, it is very difficult and inefficient to program and manage each WAP individually and manually. Typically, a wireless LAN controller (WLC) is used as a central point or controller to deploy and manage all WAPs on a wireless network. When connecting to the network, each WAP connects to its WLC to get its configuration, radio channel, transmission power, and other settings. The WAPs communicate with the WLC and send their operational

wireless information to the WLC. The WLC can then use the collective information from all its WAPs to automatically adjust settings such as user load, radio channels, and radio power to improve the performance of the wireless network.

It is important to verify that sufficient RF signal level is available for the users in a WLAN. This is best accomplished by performing a **site survey**. Inside a building, a site survey is performed to determine the best location(s) for placing the access point(s) for providing maximum RF coverage for wireless clients. Site surveys are also conducted for outside installations to determine the coverage area.

Site Survey

A process used to determine the best location(s) for placing the access point(s) to provide maximum RF coverage for wireless clients

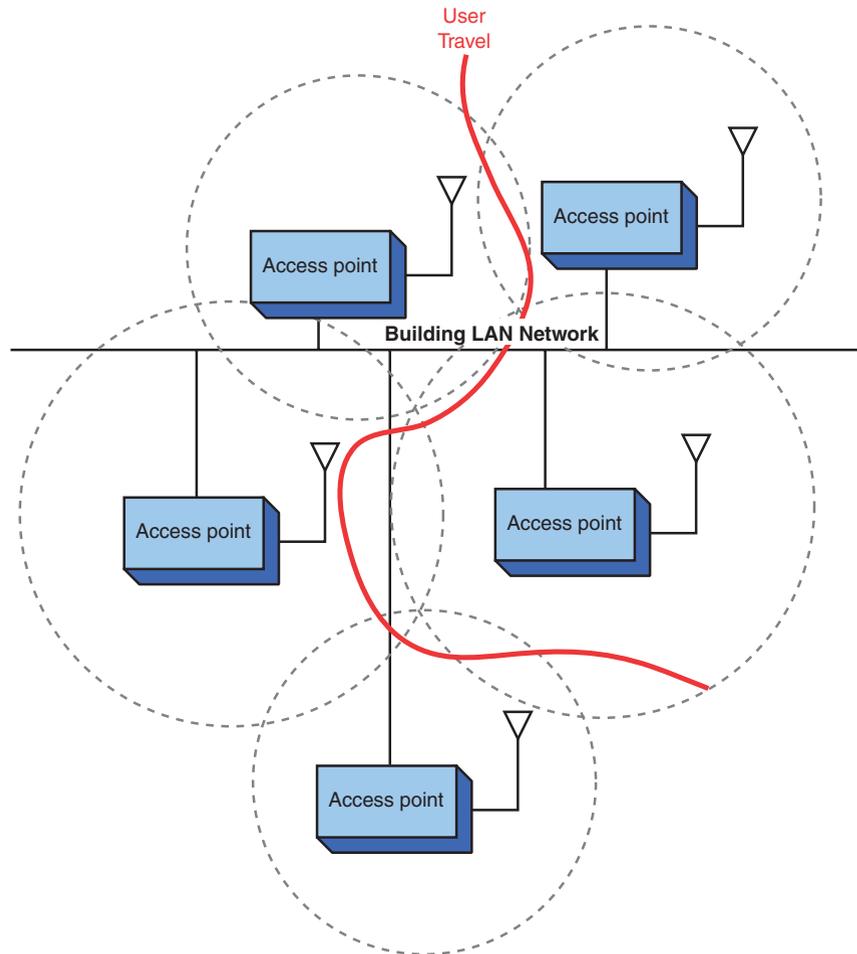


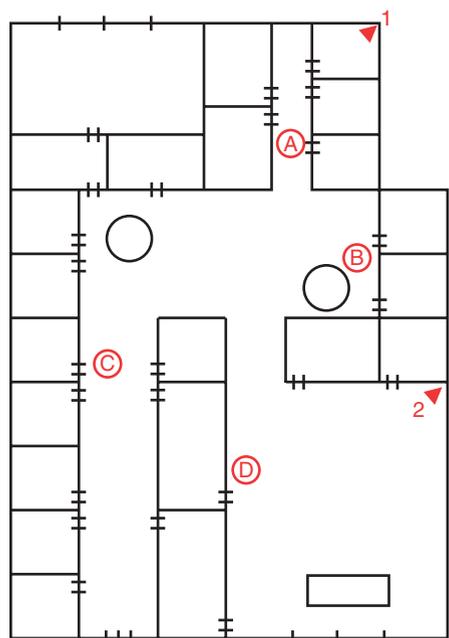
FIGURE 4-11 An example of configuring multiple access points to extend the range for wireless connectivity.

A site survey for indoor and outdoor installations should obtain the following key information:

- Indoor:
 - Electrical power
 - Wired network connection point(s)

- Access point placement
- RF coverage—user mobility
- Bandwidth supported
- Identify any significant RF interference
- Outdoor:
 - Electrical power (base access point)
 - Connection back to the home network
 - Antenna selection
 - Bandwidth supported
 - RF coverage
 - Any significant RF interference

Say that a site survey is conducted to determine access point placement to provide wireless network connectivity for the building whose floor plan is shown in Figure 4-12. The objective is to provide mobile client access throughout the building. The building already has two wired connections available for placing an access point.



▶ = Ethernet CAT5e

FIGURE 4-12 The floor plan for a building being surveyed for a wireless LAN.

The available wired network connections are indicated in the drawing in Figure 4-12. The site survey begins with placing an access point at position 1. A wireless mobile client is used to check the signal throughout the building. This checking used to be performed by a laptop with a purpose-built WLAN adapter as a Wi-Fi analyzer, but today, many more options are available. Handheld devices, such as tablets and smartphones, can be conveniently used for wireless site surveys. Their form factor and mobility are perfect for this purpose. Most of these devices are already equipped with built-in wireless chips. All they need is one of the many available wireless apps. This example shows test results gathered from an Android tablet with a free Wi-Fi analyzer app installed.

Figure 4-13 shows a snapshot of the wireless environment in the area. The graph shows the signal strength for each wireless SSID found. The signal strength is the wireless signal power level, and it is represented in $-dBm$ format, from 0 to -100 . This is the power ratio, in dB, of the measured power referenced to 1 mW. The closer the value is to 0, the stronger the signal, and the stronger the signal, the more reliable the wireless connection. Wireless is everywhere today, so when you conduct a site survey, you should not be too surprised to see more SSIDs than just yours. For this example, the site survey is intended for the wireless SSID ET377. As the graph shows, ET377 has the strongest signal of all the SSIDs. However, the signal strength may not represent the goodput. *Goodput* refers to the actual wireless data throughput, as measured by an application on the end device. It represents the actual transmission rate of a wireless connection, which is not the maximum theoretical transmission rate.

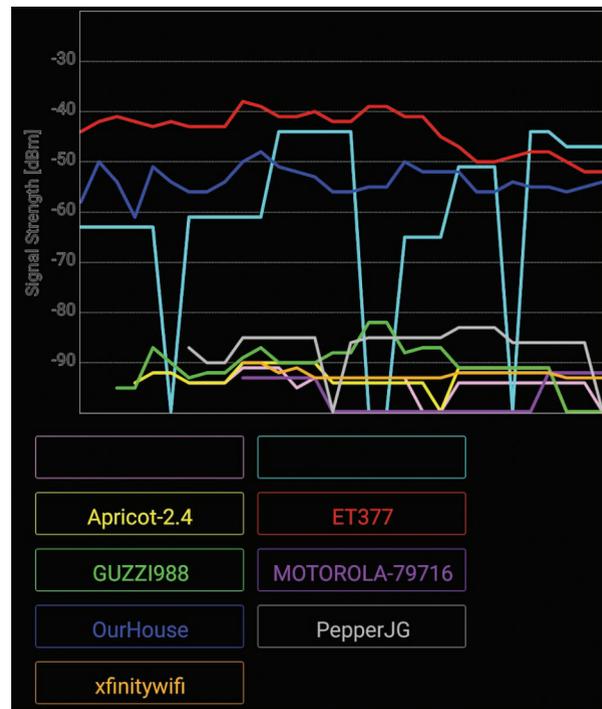


FIGURE 4-13 A snapshot of the RF signal environment.

The first measurement, shown in Figure 4-14, is taken at point A. Notice that the signal strength is at -43 dBm, which is an excellent connection. This will change if the signal level decreases significantly.

The next observation is made at point B, and the signal strength is measured at -52 dBm (see Figure 4-15). The signal has decreased somewhat, but it is still acceptable, which indicates that a connection is still good. The signal level drops to -67 dBm at point C, as shown in Figure 4-16. This connection is fair.

A floor plan showing the locations of wireless access points and wireless signal strength and coverage is a wireless or Wi-Fi heat map. Typically, a wireless/Wi-Fi heat map shows a real map of a room, floor, or even a city overlaid by a graphical representation of a wireless signal.

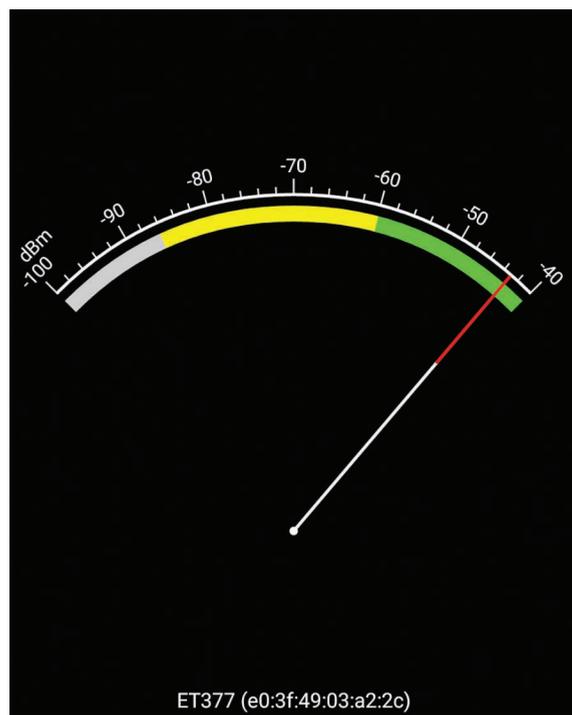


FIGURE 4-14 The RF signal strength observed at point A.

The mobile client is moved to point D in the building, and signal quality “Out of range” is observed (see Figure 4-17). This is also called a *loss of association* with the access point.

The site survey indicates that one access point placed at point 1 in the building is not sufficient to cover the building’s floor plan. The survey shows that the additional cost of another access point is easily justified for providing full building wireless LAN coverage. The building has two wired network connections available for placing an access point (points 1 and 2). It is decided to place another access point at point 2. The site survey is repeated, and it shows excellent signal strength obtained throughout the building.



FIGURE 4-15 The RF signal strength at point B.



FIGURE 4-16 The drop in the signal quality to fair at point C.

In some cases, a *range extender* can be used to provide additional wireless coverage. This device basically extends the reach of the wireless network.

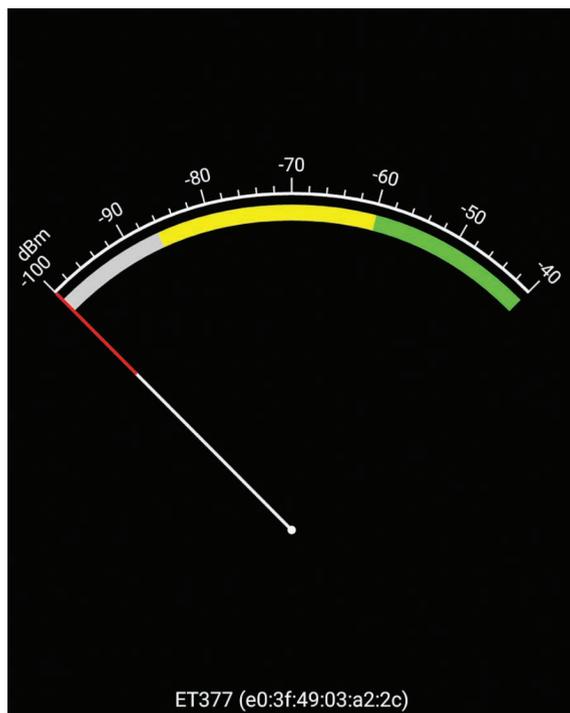


FIGURE 4-17 The “Out of range” measurement for point D.

Section 4-3 Review

This section covers the following Network+ exam objectives.

1.6 Explain the use and purpose of network services.

This section introduces the services provided by a wireless LAN adapter: delivery of the data, authentication, and privacy.

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

A physical cable connection (typically CAT6 or greater) ties an access point to a wired network’s switch or hub (typically Ethernet).

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section introduces the SSID. An 802.11 wireless LAN device uses an SSID to identify what wireless data traffic is allowed to connect to the network. The SSID is the wireless service set identifier, basically a password that enables the client to join the wireless network.

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section talks about preparing a site to support access point placement and the changes in signal strength that result from environmental factors.

3.2 Explain the purpose of organizational documents and policies.

The available wired network connections are indicated in a floor plan for a building being surveyed for a wireless LAN.

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

A site survey for indoor and outdoor installations should obtain the following key information:

- Electrical power
- Wired network connection point(s)
- Access point placement
- RF coverage—user mobility
- Bandwidth supported
- Identify any significant RF interference

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

The wrong SSID prevents an association, keeping a client from being able to become a member of the wireless network.

Test Your Knowledge

1. What happens when an *association* is made?
 - a. A wireless connection is obtained.
 - b. The MAC address of the client is obtained.
 - c. Unauthorized network access is prevented.
 - d. Excessive routing is prevented.
2. True or false: Site surveys help determine the following:
 - The best location for placing access points
 - Power connection
 - RF coverage
 - Antenna selection
 - IP address selection

True

4-4 BLUETOOTH, WIMAX, RFID, AND MOBILE COMMUNICATIONS

This section looks at four wireless technologies: Bluetooth, WiMAX, RFID, and mobile communications. These technologies all play important roles in wireless networks, and this section looks at each of them. This section also looks at configurations and examples of the hardware being used. A fun exercise is to have students connect their laptops to each other using Bluetooth, as described in the example presented in this section.

This section looks at four wireless technologies: Bluetooth, WiMAX, RFID, and mobile communications. Each of these technologies plays an important role in wireless networks. The sections that follow examine each of these wireless technologies, including a look at configuration and examples of the hardware being used.

Bluetooth

The wireless technology Bluetooth is based on the 802.15 standard. Bluetooth was developed to replace the cable connecting computers, mobile phones, handheld devices, portable computers, and fixed electronic devices. The information normally carried by a cable is transmitted over the 2.4GHz ISM frequency band, which is the same frequency band used by 802.11b/g/n/ax. There are four output power classes for Bluetooth. Table 4-6 lists the maximum output power and the operating distance for each class.

Bluetooth Low Energy (BLE) technology has been developed to provide operation on a small battery for up to five years. This technology is ideal for applications that require the exchange of small amounts of data periodically. BLE operates in the 2.4GHz ISM band and remains in sleep mode except when a connection is initiated. BLE devices have significantly lower power requirements than do traditional Wi-Fi devices. For example, whereas a Wi-Fi device consumes about 500 μW for 10 messages, a BLE device consumes only 50 μW .

TABLE 4-6 Bluetooth Output Power Classes

Power Class	Average Output Power	Operating Distance
1	100 mW	~100 meters
2	2.5 mW	~10 meters
3	1 mW	~1 meter
4	0.5 mW	~0.5 meter

When a Bluetooth device is enabled, it uses an **inquiry procedure** to determine whether any other Bluetooth devices are available. The device also uses this procedure to allow itself to be discovered.

If a Bluetooth device is discovered, it sends an inquiry reply back to the Bluetooth device initiating the inquiry. Next, the Bluetooth devices enter the **paging procedure**, which is used to establish and synchronize a connection between

Inquiry Procedure

A process used to determine whether other Bluetooth devices are available

Paging Procedure

A process used to establish and synchronize a connection between two Bluetooth devices

Piconet

An ad hoc network of up to eight Bluetooth devices

Pairing

Setting up a Bluetooth device to connect to another Bluetooth device

Passkey

A passphrase used in Bluetooth security to limit outsider access to pairing

two Bluetooth devices. When the procedure for establishing the connection has been completed, the Bluetooth devices will have established a **piconet**, an ad hoc network of up to eight Bluetooth devices, such as a computer, mouse, headset, earpiece, and so on. In a piconet, one Bluetooth device (the primary) is responsible for providing the synchronization clock reference. All other Bluetooth devices are called *secondaries*.

Let's look at an example of setting up a Bluetooth network linking a macOS computer to another Bluetooth-enabled device. To enable Bluetooth on macOS, click **Apple icon > System Preferences > Bluetooth** and then click **Turn Bluetooth On** (see Figure 4-18). The Mac automatically discovers other Bluetooth devices nearby.

Next, you need to select the device with which you will be establishing a Bluetooth connection. When Bluetooth is turned on, the Mac searches for another Bluetooth device. When a Bluetooth device is found, it appears in the Devices window. To connect the desired Bluetooth device, select the **Pair** button next to the device. (The process of setting up a Bluetooth device to connect to another Bluetooth device is called **pairing**.) You are asked for a passkey or passphrase. The **passkey** is used in Bluetooth security to limit outsider access to the pairing. Only people with the passkey can pair with the Bluetooth device. Anyone who tries to pair units with the wrong passphrase will not be able to pair.

At this point, you can transfer files between the paired devices if the Bluetooth Sharing settings for the device have been set to allow files to come in. Find these settings by clicking **Apple icon > System Preferences > Sharing** and selecting **Bluetooth Sharing**. Figure 4-19 shows an example of the setup for the file transfer.

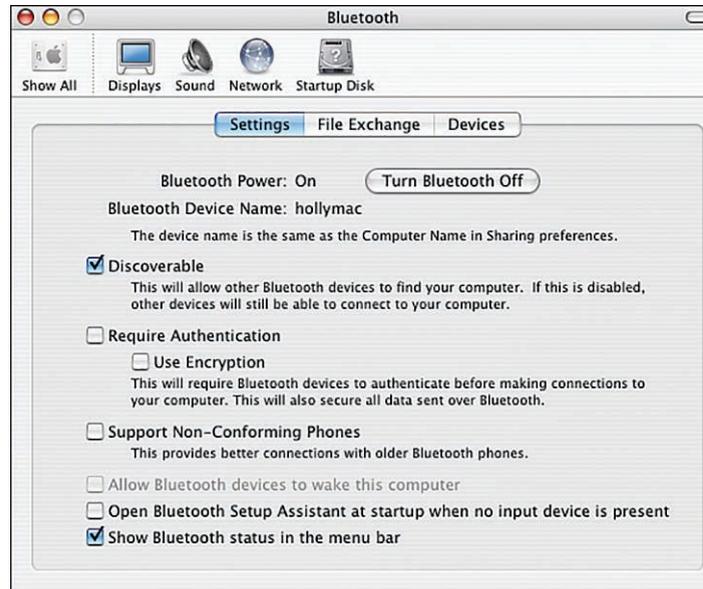


FIGURE 4-18 The window for configuring Bluetooth settings on a Mac.

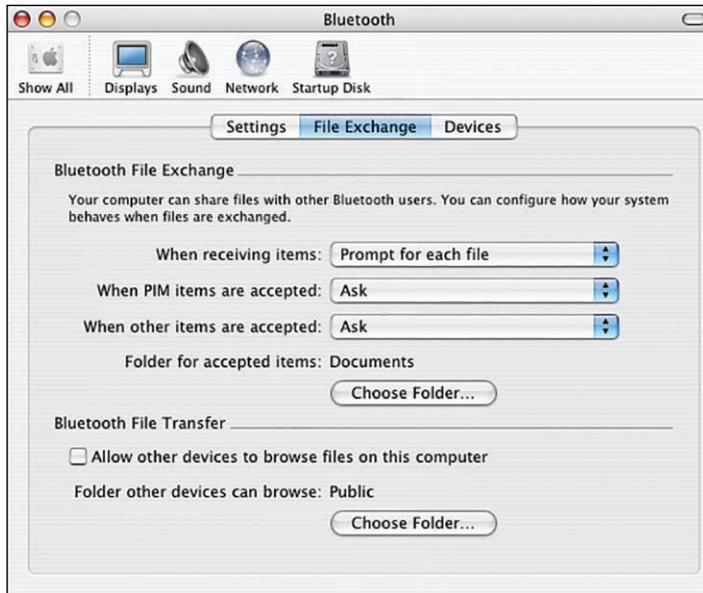


FIGURE 4-19 The Mac window showing the settings for a file transfer.

Figure 4-20 shows an incoming text file. The File Transfer menu enables you to select where received files are saved. In this case, the incoming files are being saved to the desktop.

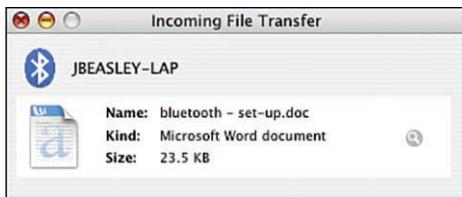


FIGURE 4-20 The Mac window showing that a text file is coming in from another Bluetooth device.

The details for setting up Bluetooth on Windows 10 differ slightly from those for macOS, but the basic steps are the same:

1. Enable the Bluetooth radio.
2. Enable discoverability (to allow other Bluetooth devices to find the device).
3. Select the device for pairing.

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is a broadband wireless system that has been developed for broadband wireless access (**BWA**) for fixed

WiMAX

Worldwide Interoperability for Microwave Access, a broadband wireless system based on the IEEE 802.16e standard

BWA

Broadband wireless access

and mobile stations and can provide a wireless alternative for last-mile broadband access in the 2GHz–66GHz frequency range. BWA access for fixed stations can be up to 30 miles, whereas mobile BWA access is 3–10 miles. Internationally, the WiMAX frequency standard is 3.5GHz, while the United States uses both the unlicensed 5.8GHz and the licensed 2.5GHz spectra. In addition, WiMAX has been investigatively adapted for use in the 700MHz frequency range. Information transmitted at this frequency is less susceptible to signal blockage due to trees. The disadvantage of the lower frequency range is the reduction in bandwidth.

NLOS

Non-line-of-sight

WiMAX uses OFDM as its signaling format. This signaling format was selected for the WiMAX IEEE 802.16a standard because of its improved **NLOS** (non-line-of-sight) characteristics in the 2GHz–11GHz frequency range. An OFDM system uses multiple frequencies for transporting the data, which helps minimize multipath interference problems. Some frequencies may experience interference problems, but the system can select the best frequencies for transporting the data.

WiMAX also provides flexible channel sizes (for example, 3.5MHz, 5MHz, and 10MHz), which provides adaptability to standards for WiMAX worldwide. This also helps ensure that the maximum data transfer rate is supported. For example, the allocated channel bandwidth could be 6MHz, and the adaptability of the WiMAX channel size enables it to adjust to use the entire allocated bandwidth.

In addition, the WiMAX (IEEE 802.16e) media access control (MAC) layer differs from the IEEE 802.11 Wi-Fi MAC layer in that the WiMAX system has to compete only once to gain entry into the network. When a WiMAX unit has gained access, the base station allocates a time slot to it, thereby providing the WiMAX system scheduled access to the network. The WiMAX system uses time-division multiplexing (TDM) data streams on the downlink and time-division multiple access (TDMA) on the uplink and centralized channel management to ensure that time-sensitive data is delivered on time. In addition, WiMAX operates in a collision-free environment, which improves channel throughput.

Last Mile

The last part of the connection from a telecommunications provider to a customer

WiMAX has a range of up to 30 miles, and it operates in both point-to-point and point-to-multipoint configurations. This can be useful in situations where DSL or cable network connectivity is not available. WiMAX is also useful for providing the last-mile connection. The **last mile** is basically the last part of the connection from a telecommunications provider to a customer. The cost of the last mile connection can be high, which makes a wireless alternative attractive to customers.

Radio Frequency Identification (RFID)

A technique that uses radio waves to track and identify people, animals, objects, and shipments

Backscatter

The reflection of radio waves striking an RFID tag and reflecting back to the transmitter source

The 802.16e WiMAX standard holds a lot of promise for use as a mobile air interface.

Radio Frequency Identification

Radio frequency identification (RFID) uses radio waves to track and identify people, animals, objects, and shipments. It is based on the principle of modulated **backscatter**—the reflection of the radio waves striking an RFID tag back to the transmitter source, with its stored unique identification information.

Figure 4-21 illustrates a basic RFID system, which consists of two elements:

- **RFID tag:** An RFID tag (also called an RF transponder) includes an integrated antenna and radio electronics.

- **Reader:** A reader (also called a transceiver) consists of a transceiver and an antenna. A transceiver is a combination of a transmitter and receiver.

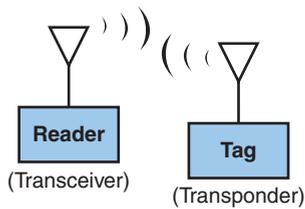


FIGURE 4-21 Basic block diagram of an RFID system.

The reader transmits radio waves, which activates (turns on) an RFID tag. The tag then transmits modulated data, containing its unique identification information stored in the tag, back to the reader. The reader then extracts the data stored on the RFID tag.

The RFID idea dates back to 1948, when the concept of using reflected power as a means of communication was first proposed. The 1970s saw further development in RFID technology—in particular, a UHF scheme that incorporates rectification of the RF signal for providing power to the tag. Development of RFID technology significantly increased in the 1990s. Applications included toll collection that allowed vehicles to pass through tollbooths at highway speeds while still being able to record data from the tag.

Today, RFID technology is being used to track inventory shipments for major commercial retailers, by the transportation industry, and by the Department of Defense. In addition, RFID applications are being used in Homeland Security for tracking container shipments at border crossings. In addition, RFID is being incorporated into WLAN computer networks to keep better track of inventory. RFID technology is being used as a wireless means of asset tracking and is therefore becoming more important in networks. The tracking technology is even being extended to tracking Wi-Fi devices within the WLAN infrastructure.

Three parameters define an RFID system:

- Means of powering the tag
- Frequency of operation
- Communications protocol (also called the air interface protocol)

Powering the Tag RFID tags are classified in three ways, based on how they obtain their operating power:

- **Passive:** Power is provided to a passive tag by rectifying the RF energy, transmitted from the reader, that strikes the RF tag antenna. The rectified power level is sufficient to power the ICs on the tags and also provides

sufficient power for the tag to transmit a signal back to the reader. Figure 4-22 shows an example of a passive RFID tag (also called an inlay). A tag inlay includes both an RFID chip and an antenna mounted on a substrate.

- **Semi-active:** With semi-active tags, a battery powers the electronics on a tag, but the tag uses backscatter to transmit information back to the reader.
- **Active:** With active tags, a battery powers the tag and transmits a signal back to the reader. Basically, this is a radio transmitter. New active RFID tags are incorporating wireless Ethernet (that is, 802.11 Wi-Fi connectivity). An example is the G2C501 active RFID tag from G2 Microsystems, shown in Figure 4-23. The power consumption of the G2C501 is 10 μ A in sleep mode, and the device uses two AA batteries with an expected lifetime of five years. The G2C501 also works in the standard 915MHz range. In addition, the G2C501 has location capability. This is accomplished by making receive signal strength indicator (RSSI) measurements from three separate access points. The three measurements provide sufficient information to make a triangulation measurement for use in locating the object.

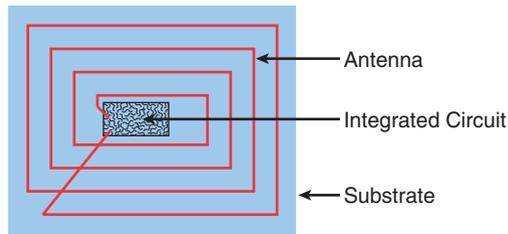


FIGURE 4-22 An example of an RFID inlay.

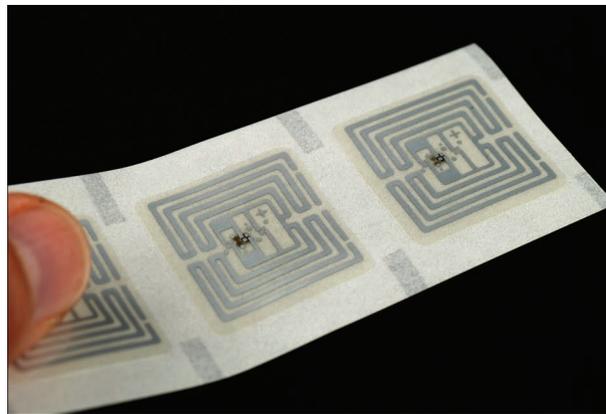


FIGURE 4-23 The G2C501 active RFID tag from G2 Microsystems (Albert Lozano/Shutterstock).

Frequency of Operation RFID tags must be tuned to the reader's transmit frequency in order to turn on. RFID systems typically use three frequency bands for operation (see Figure 4-24):

- **Low frequency (LF):** LF tags typically use frequency-shift keying (FSK) between the 125KHz and 134KHz frequencies. These tags can handle only low data rates (~12Kbps), and they are not appropriate for any applications requiring fast data transfers. However, LF tags are suitable for animal identification, such as with dairy cattle and other livestock. The RFID tag information is typically obtained when the livestock are being fed. The read range for low-frequency tags is approximately 0.33 meter.
- **High frequency (HF):** HF tags operate in the 13.56MHz industrial band. High-frequency tags have been available commercially since 1995. The longer wavelengths of the HF radio signal are less susceptible to absorption by water or other liquids. Therefore, these tags are suitable for tagging liquids. The read range for HF tags is approximately 1 meter. The short read range provides for better-defined read ranges. The applications for tags in this frequency range include access control, smart cards, and shelf inventory. The data rate for HF tags is 26Kbps.
- **Ultra-high frequency (UHF):** UHF tags work at 860–960MHz and at 2.4GHz. The data rates for these tags can be 50–150Kbps and greater. These tags are popular for tracking inventory. The read range for passive UHF tags is 3–6 meters, which makes them a good choice for reading pallet tags. However, if an active tag is used, a read range up to 100 meters is possible.

LF	HF	UHF
125/134 kHz	13.56 MHz	860–960 MHz 2.4 GHz

FIGURE 4-24 The frequency bands used by RFID tags.

Communications (Air Interface) Protocol The air interface protocol adopted for RFID tags is **Slotted Aloha**, a network communications protocol similar to the Ethernet protocol. With Slotted Aloha, the tags are only allowed to transmit at predetermined times after being energized. This technique reduces the likelihood of data collisions between RFID tag transmissions and allows for the reading of up to 1000 tags per second (for high-frequency tags). The operating range for RFID tags can be up to 30 meters. This means that multiple tags can be energized at the same time, and RF data collisions can possibly occur. If a collision occurs, the tag will transmit again after a random back-off time. The readers transmit continuously until there is no tag collision.

Slotted Aloha

A wireless network communications protocol similar to the Ethernet protocol

Mobile (Cellular) Communications

Today, many types of mobile devices, also called cellular devices, can be used to access computer networks. Examples include smartphones, laptops, tablets, and gaming devices. All of these devices are extremely powerful and use wireless technology to connect to the network. This chapter has provided an overview of many of the wireless technologies being used today, including the 802.11 family of Wi-Fi technologies, Bluetooth, WiMAX, and RFID. This section provides a brief summary of some of the other wireless technologies currently available.

CDMA CDMA (code-division multiple access) is a communications technology in which spread-spectrum techniques are used to multiplex more than one signal within a single channel. In this case, each device uses a different binary sequence to modulate the carrier, spreading the spectrum of the waveform (spread spectrum). The signals are separated at the receiver by a correlator that accepts only the signal from the selected binary sequence.

LTE/4G LTE (Long Term Evolution) is a 4G wireless communications standard. It is designed to provide speeds up to 10 times those of 3G networks.

HSPA+ HSPA+ (Evolved High-Speed Packet Access) provides network speeds comparable to those of LTE networks. Theoretical speeds are 168Mbps for download and 22Mbps uplink.

3G/4G/5G 3G (Third Generation) was developed to provide broadband network wireless services. The standard defining 3G wireless is International Mobile Communications, or IMT 2000. 4G (Fourth Generation), which is the successor to 3G technology, provides download speeds of 100Mbps. 5G (Fifth Generation) is the latest wireless network technology provided by the cellular network, with speeds ranging from 40Mbps to 1.5Gbps.

EDGE EDGE (Enhanced Data GSM Evolution) provides download speeds of 384Kbps.

NFC A concept related to mobile communications and smartphones is NFC, which stands for Near Field Communication. NFC is a set of communication protocols that are used to enable two electronic devices to communicate. A typical NFC device is a smartphone. By using NFC, smartphones can establish communication if they are within 4 cm of each other. Applications of NFC include reading electronic tags and making payments.

Geofencing With many type of wireless devices using different type of wireless technologies, it has become more and more difficult for network administrators to keep track of the devices entering and leaving the premises. *Geofencing* is used to create a virtual electronic boundary for mobile and wireless devices to detect their whereabouts as well as control certain functionalities, such as camera or microphone, of the devices through the use of mobile device management (MDM). For example, geofencing may be used in a highly classified area or a restricted area in a corporate building.

Section 4-4 Review

This section covers the following Network+ exam objectives.

- 1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

This section introduces the RFID reader, which consists of a transceiver and an antenna. A transceiver is a combination of a transmitter and receiver.

- 1.7 Explain basic corporate and datacenter network architecture.

This section introduces Bluetooth, RFID, WiMAX, and mobile can support links up to 30 miles and is a possible alternative for providing last-mile connections.

- 2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section introduces geofencing, which is used to create a virtual electronic boundary for mobile and wireless devices to detect their whereabouts as well as control certain functionalities, such as camera or microphone, of the devices through the use of mobile device management (MDM).

- 2.3 Given a scenario, configure and deploy common Ethernet switching features.

This section introduces 5G (Fifth Generation), which is the latest wireless network technology provided by the cellular network, with speeds ranging from 40Mbps to 1.5Gbps.

- 2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section introduces Bluetooth, RFID, WiMAX, and mobile technologies.

- 3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

This section examines the download speeds for many different technologies.

- 4.3 Given a scenario, apply network hardening techniques.

This section introduces the concept of geofencing.

- 5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

This section mentions that WiMAX operates in a collision-free environment, which improves channel throughput.

- 5.5 Given a scenario, troubleshoot general networking issues.

The air interface protocol adopted for RFID tags is Slotted Aloha, a network communications protocol similar to the Ethernet protocol. With Slotted Aloha, tags are only allowed to transmit at predetermined times after being energized. This technique reduces the likelihood of data collisions between RFID tag transmissions and allows for the reading of up to 1000 tags per second (for high-frequency tags).

Test Your Knowledge

1. WiMAX operates at which frequencies in the United States?
 - a. Both the unlicensed 5.2GHz and the licensed 2.4GHz spectra
 - b. Both the unlicensed 5.3GHz and the licensed 2.6GHz spectra
 - c. Both the unlicensed 13.2GHz and the licensed 5.6GHz spectra
 - d. Both the unlicensed 5.8GHz and the licensed 2.5GHz spectra
2. What is the maximum range of WiMAX?
 - a. 30 kilometers
 - b. 30 miles
 - c. 30 meters
 - d. None of these answers are correct.
3. At what frequency does Bluetooth operate?
 - a. 5GHz
 - b. 100MHz
 - c. 2.4GHz
 - d. None of these answers are correct.

4-5 CONFIGURING A POINT-TO-MULTIPOINT WIRELESS LAN: A CASE STUDY

This section presents an example of preparing a proposal for providing a point-to-multipoint wireless network for a company. It walks through the multiple steps involved in implementing a point-to-multipoint wireless network, including performing an antenna site survey, establishing a link to the home network, configuring the multipoint distribution, and configuring the remote site.

This section presents an example of preparing a proposal for providing a point-to-multipoint wireless network for a company. The administrators for the company have decided that it would be beneficial to provide a wireless network connection for their employees back to the company's network (the home network). This example walks through the following steps:

1. Conducting an initial antenna site survey
2. Establishing a link from the home network to the distribution point
3. Configuring the multipoint distribution
4. Conducting an RF site survey for establishing a baseline signal level for the remote wireless user
5. Configuring the remote user's installation

The objective of this example is to establish a point-to-multipoint wireless network that provides remote users with a wireless network connection. The remote users are to be at fixed locations within the proposed coverage area. Figure 4-25 shows a simple terrain profile of the proposed area. The data rate for the wireless connection to remote users needs to be at least 2Mbps.

Note

Antenna placement is critical when setting up a point-to-multipoint wireless LAN. Incorrect antenna placement can severely affect reception quality.

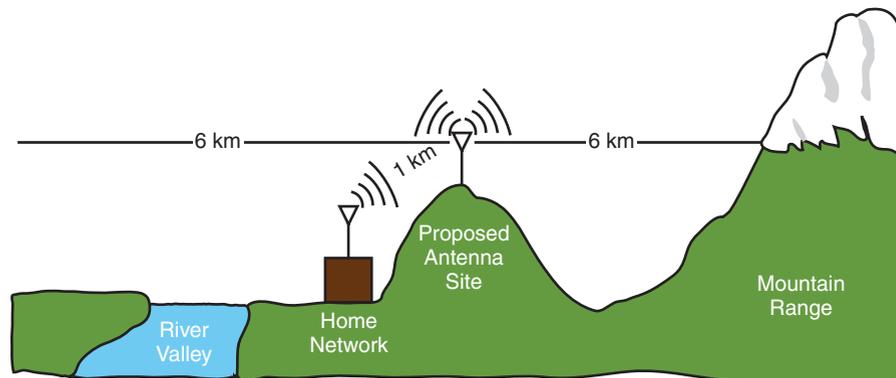


FIGURE 4-25 The terrain profile of the area to be supported by the proposed point-to-multipoint wireless network.

Step 1: Conducting an Antenna Site Survey

The proposed antenna site (refer to Figure 4-25) is on top of a hill approximately 1 kilometer from the home network. A site survey provides the following information:

- The site has a tower that can be used to mount the wireless antenna.
- The site has a small building and available rack space for setting up the wireless networking equipment.
- There is a clear view of the surrounding area for 6 kilometers in every direction.
- There is not an available wired network connection back to the home network. The decision is made to use the proposed antenna site and set up an 11Mbps wireless link back to the home network.

Step 2: Establishing a Point-to-Point Wireless Link to the Home Network

The cost of installing a wired connection back to the home network would be too high, so it is decided to use a point-to-point 802.11 wireless link for the interconnection. This requires that antennas be placed at both the home network and the antenna site. A wireless bridge is used at each end of the point-to-point wireless link to interconnect the networks. The bridge will connect to the wired home network and to the multipoint distribution on the antenna site. Also, each antenna will be outfitted with lightning arrestors to protect the electronics from any possible lightning strikes. Figure 4-26 shows the proposed wireless connection.

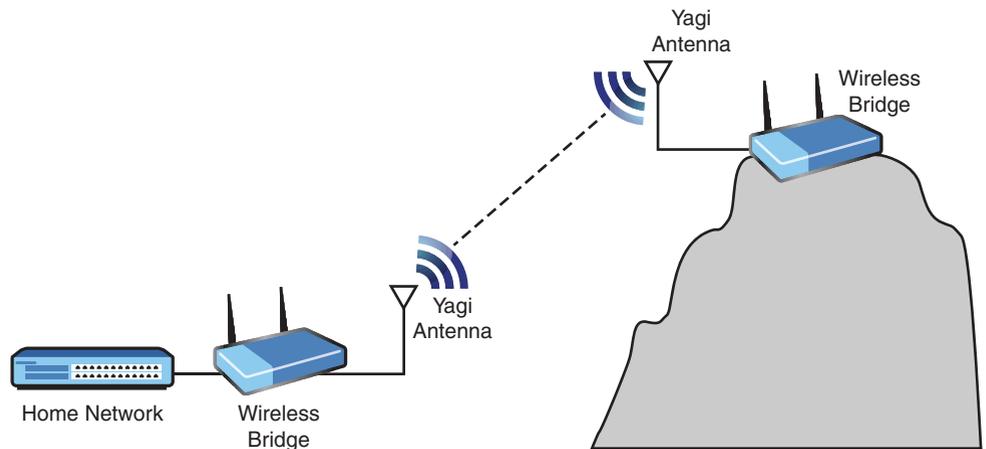


FIGURE 4-26 The proposed point-to-point wireless link between the home network and the antenna site.

Many manufacturers of antennas support wireless networking, and many types of antenna can be used. Antenna types from many manufacturers were investigated for possible use in the interconnection. Three possible antennas were selected for the wireless network, as outlined in Table 4-7.

Note

The selection of the incorrect antenna type can lead to a poorly designed radio link and poor reliability.

TABLE 4-7 Sample of 802.11 Wireless Antennas

Antenna	Type	Radiation Pattern	Costs
A	Omni	Omnidirectional	Moderate
B	Yagi	Directional	Moderate
C	Dish	Highly directional	High

Antenna A has an omnidirectional radiation pattern. This means the antenna can receive and transmit signals in a 360-degree pattern. Figure 4-27(a) shows the radiation pattern for an omnidirectional antenna. Antenna A supports all 802.11 types. Table 4-7 also indicates that this antenna has a moderate cost.

Antenna B is a Yagi antenna with a directional or unidirectional radiation pattern, as shown in Figure 4-27(b). The Yagi antenna supports all 802.11 antenna types.

Antenna C is a dish antenna, or parabolic reflector. These antennas provide extremely high directional gain, as illustrated in Figure 4-27(c). The dish antenna supports 802.11 systems. The cost of a dish antenna can be quite high relative to the cost of a Yagi or an omnidirectional antenna.

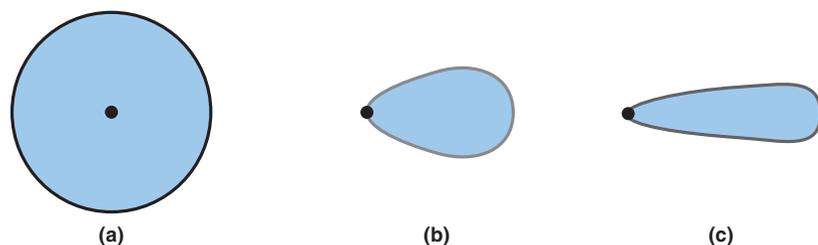


FIGURE 4-27 Antenna radiation patterns for (a) omnidirectional, (b) Yagi, and (c) dish [parabolic reflector] antennas. The cost of the Yagi antenna is comparable to that of the omnidirectional antenna.

Antenna B, the directional Yagi, is selected for the point-to-point link. The antenna meets the distance requirement and also meets the 11Mbps data rate requirement. Antennas A and C were not selected for the following reasons:

- **Antenna A:** The omnidirectional radiation pattern is not appropriate.
- **Antenna C:** The cost of a high-gain dish antenna is not justified for the short distance.

Steps 3 and 4: Configuring the Multipoint Distribution and Conducting an RF Site Survey

At this point, a wireless data link has been established with the home network. The next task is to configure the antenna site for multipoint distribution. It was previously decided that a 300Mbps link would be adequate for the remote users, based on the data rate to be supported for the planned coverage area.

The site survey in step 1 showed that there is a clear view of the surrounding area for 6 kilometers in each direction. Antenna A (see Table 4-7) provides an omnidirectional radiation pattern for 7 kilometers. This satisfies the coverage area. Antenna A is mounted on the antenna site tower, connected to a lightning arrestor,

and then connected to the output of a wireless bridge. Next, an RF site survey of the planned coverage area is conducted to verify the signal quality provided by the antenna selected. Measurements are made from multiple locations in the planned coverage area. All remote sites within 4 kilometers of the distribution show excellent signal strength (see Figure 4-28).

The signal quality drops to good at 6 kilometers at all surveyed remote locations except for one area, which shows a poor quality (see Figure 4-29). The signal is apparently being affected by multipath distortion from a small lake area. A fix to this might be to move the antenna to a different height to minimize reflection problems. An antenna at a different height will receive different reflections and possibly less interference. In some cases, antenna alignment can be changed to decrease the interference. A more costly solution would be to add antenna diversity, which basically means placing multiple antennas on the receiving tower and using the best signal for the connection.

Note

When dealing with antennas, it is important to consider effective isotropic radiated power (EIRP), which is the power that comes off an antenna and is the value the FCC uses to determine and measure power limits in wireless equipment.

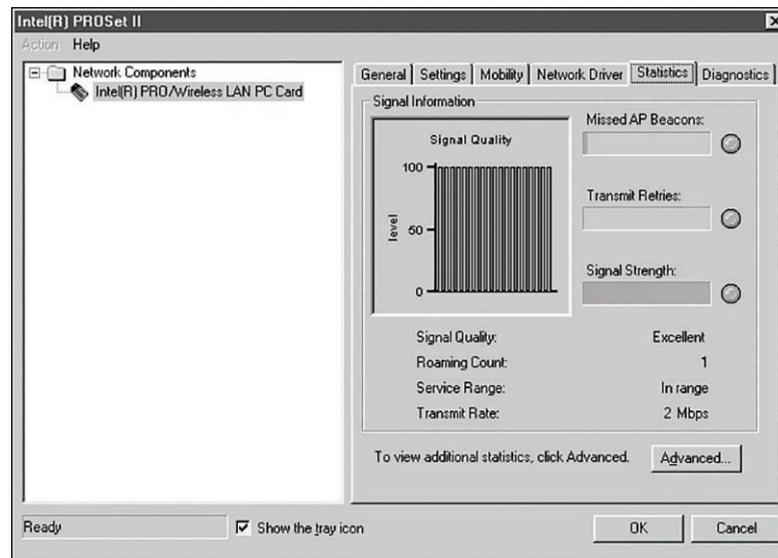


FIGURE 4-28 The excellent signal quality measured for the multipoint distribution.

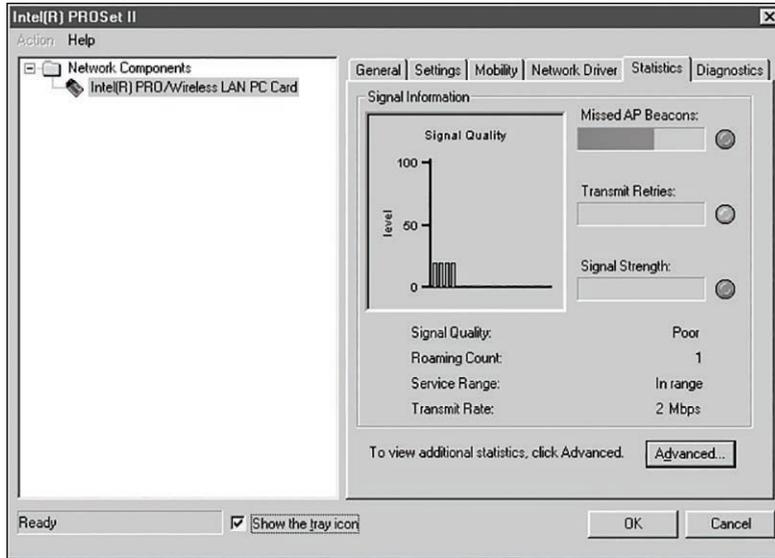


FIGURE 4-29 The poor signal quality measured at the remote site near the lake.

Step 5: Configuring the Remote Installations

The last task is to develop a configuration for the remote users. The antenna for each remote user needs to be able to see only the multipoint distribution antenna site. The requirements for the remote client are as follows:

- 300Mbps data rate connection
- Directional antenna (Yagi) plus mount, lightning arrestor, and wireless bridge

Antenna B (refer to Table 4-7) is selected for the directional antenna. This antenna will provide a sufficient RF signal level for the remote users. Each remote user will need a wireless bridge and a switch to connect multiple users. (Note that the bridge is set for a 2.4Mbps data rate.) Figure 4-30 shows the setup for the remote users.

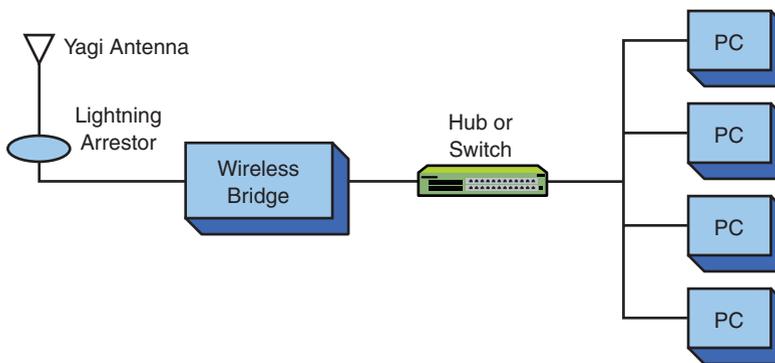


FIGURE 4-30 The setup for the remote users in the proposed point-to-multipoint wireless network.

Section 4-5 Review

This section covers the following Network+ exam objectives.

- 2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

This section examines various networking devices for establishing wireless networks.

- 2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

This section presents various types of antennas that can be used to develop a wireless network.

- 3.2 Explain the purpose of organizational documents and policies.

This section introduces the steps for completing a wireless antenna site survey.

- 3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

This section discusses a situation in which the signal is being affected by multipath distortion from a small lake area. A fix to this might be to move the antenna to a different height to minimize reflection problems.

- 4.3 Given a scenario, apply network hardening techniques.

This section discusses the issues related to and planning for antenna placement.

- 5.4 Given a scenario, troubleshoot common wireless connectivity issues.

This section presents antenna types and placement.

Test Your Knowledge

1. Which types of antennas are typically used at receive sites from a multipoint distribution system? (Select all that apply.)
 - a. Yagi
 - b. Omnidirectional
 - c. Parabolic
 - d. Hydroxyl
2. True or false: When configuring remote installations for wireless networks, the receive site needs to be able to see the multipoint distribution antenna site.

True

4-6 TROUBLESHOOTING WIRELESS NETWORKS

This section provides an overview of common techniques for troubleshooting wireless networks. Students should become familiar with each scenario presented.

This section examines some common techniques for troubleshooting wireless networks. Wireless networks have greatly simplified the steps for connecting to a network, but they do occasionally fail. The following sections describe some scenarios that users might encounter and steps for troubleshooting and resolving the wireless issues.

Access Point Hardware Issues

The primary hardware device in wireless networks is the access point. Some networks have multiple access points. A simple first step is to ping the IP address for an access point in order to verify network connectivity. You should expect a reply to the ping, but if you don't get a reply, you can verify the IP address and repeat the ping. If it still doesn't work, there is a good chance there is a problem with the access point. Try unplugging the access point and plugging it back in to reset the access point. Try the ping again, and if it still doesn't work, the access point might have a problem.

Wireless Router Issues

Make sure the client and wireless router support the same Wi-Fi version. For example, if a client computer's Wi-Fi card supports only 802.11b, the wireless router must also support 802.11b or must be configured to run in a mixed mode, with multiple protocols supported.

Also, in the case where multiple clients are connecting to the wireless router, it is important to understand that when an association is made between the client and the wireless router, the client with the lowest 802.11 system will set the clock speed. For example, say that a client running 802.11b and another running 802.11g connect to the same wireless router. The data transfer rate for 802.11b is 11Mbps, and the rate for 802.11g is 54Mbps. The wireless router will select 802.11b's lower clock rate for all associations. This can be of some concern to clients that have the capability to connect at a higher data transfer rate.

Wireless Compatibility

Not all wireless clients are created equal, and wireless clients depend on their hardware and software, which they must keep up to date. Also, in order to have reliable and good wireless connectivity, the wireless access point and the wireless clients must be compatible and use the same standard.

802.11n is a standard that can offer connectivity in either 2.4GHz or 5GHz or both. This means a wireless client can be 802.11n compatible just by operating in one frequency, not both. Therefore, an 802.11n wireless client with only a 2.4GHz radio will never achieve the high speed of 300Mbps offered by 5GHz. When troubleshooting the RF spectrum associated with a signal such as a Wi-Fi signal, a spectrum analyzer is typically used.

Signal Strength Problems

The purpose of measuring signal strength is to verify that you have good signal level at the receive location. Typically, the signal strength of a wireless connection can be adjusted at the access point to expand or reduce the area of coverage. Things change, and a loss in signal strength might not be a problem with the access point. It is possible that something could have been moved and is physically blocking the signal, thus causing RF attenuation. The RSSI (received signal strength indicator) value of a user should be monitored to identify signal strength issues.

Wireless Coverage

A wireless coverage area, or a cell, is very dependent on the RF transmission radiated from a wireless router or an access point. So, there is a limitation to the size of a cell for each access point. In a large geographic area, multiple wireless access points are deployed to create multiple cells in an attempt to give enough total coverage area. Good coverage depends on cells overlapping. Failure of cells to overlap introduces weak or dead wireless spots, thus creating insufficient wireless coverage. Also, bad coverage negatively affects client roaming. When a wireless client moves from one cell to another, it must establish an association with the new access point. With bad coverage, the AP association time increases, in turn causing delay or interruption.

Extending the Wireless Range

Another way to improve wireless coverage is to extend the wireless range. The following are general tips for extending the wireless range:

- Make sure the antenna is placed high and is not obstructed by any metal. It is important to remember that radio waves reflect off metal surfaces. Also, surfaces such as concrete and brick attenuate the signal.
- In some cases, you might have to use a high-gain antenna to help boost the receive signal strength.

Frequency Interference Problems

An electrical device such as a microwave oven may cause interference. Microwave ovens operate at the 2.4GHz frequency, which is the same band in which 802.11b/g/n devices operate. It is good to have a baseline measurement of the signal strength expected at each location in order to better identify interference. A good indicator of interference is the signal-to-noise RATIO (SNR).

Wireless Channel Utilization

For the 2.4GHz wireless frequency, the default channel for 802.11b, 802.11g, and 802.11n wireless routers is channel 6. If you have interference problems, there may be a wireless router nearby with an SSID using the same channel. In such a case, you can change the channel to 1 or 11 so that the RF spectra on these channels do

not overlap (refer to Figure 4-4). 802.11b, 802.11g, and 802.11n wireless routers have 11 possible channels, and you can select an alternate channel via the wireless router's settings. Changing to a different channel will reduce the SNR, which is likely to solve your problem. Even though 5GHz wireless has more channels, the same concept applies for 802.11a, 802.11n (5GHz), 802.11ac, and 802.11ax.

Load Issues

Wireless users share the same frequency channel to communicate to the same access point. If too many users connect to the same access point at the same time, they start experiencing slowness and packet drops due to overcapacity. For optimum load capacity, consult the documentation of the access point manufacturer.

SSID Issues

Once the SSID has been configured for a computer, it normally does not require reconfiguration. However, while traveling, you might reconfigure the SSID to connect to a different network. Also, when manually configuring an incorrect SSID or settings, human-error mistakes can be made. The simple fix is to reset the SSID when you return to your home network.

Securing Wi-Fi Issues

Any time you are connecting a wireless device to a public hotspot, there is a chance that someone using a packet sniffer will be able to see your data traffic. You can avoid possible problems by enabling WPA to secure your data traffic. Most wireless systems support multiple network security protocols (for example, different versions of WPA3, WPA2, WPA, or WEP). Make sure the client and access point are running the same security mode. Otherwise, an encryption protocol mismatch will occur, resulting in no wireless connection.

Cable Issues

Even when you are focusing on troubleshooting wireless issues, a problem could be due to a simple physical cable connection. A cable could be loose, may have become disconnected, or may be bad. It is always good to have a spare cable just in case. Remember that you can always verify that you have a connection by checking for the presence of a link light. Also, bad cables create attenuation and introduce loss of signal. Attenuation in any type of cable connecting to the access point—such as antenna cable attenuation, fiber cable attenuation, or Ethernet cable attenuation—could introduce signal issues into the wireless connection.

Deauthentication/Disassociation Attacks

Deauthentication and disassociation are legitimate handshakes used by a wireless client when leaving a wireless network. However, a denial of service (DOS) attack that exploits deauthentication and disassociation creates client disassociation issues. By spoofing a disassociate or deauthenticate message while pretending to be a targeted wireless client, the access point disassociates the targeted wireless client from the wireless network.

DHCP Issues

Wireless devices require valid IP addresses. Access points typically assign a 192.168.0.x address to the client. You can verify the IP address assigned by entering the command **ipconfig** at the command prompt (refer to Section 1-4, “The Ethernet LAN,” in Chapter 1, “Introduction to Computer Networks”).

Wireless Printer Issues

If you are experiencing problems with a wireless printer that was recently working, the first step is to restart the printer, your computer, and your wireless router. If this doesn't fix the problem, you can print the network configuration from the printer. Check the IP address for the printer and verify that it is assigned an IP address in your network. You can check the IP address of your computer by issuing the command **ipconfig** from the command prompt (refer to Section 1-4 in Chapter 1).

Section 4-6 Review

This section covers the following Network+ exam objective.

5.4 Given a scenario, troubleshoot common wireless connectivity issues. *This section presents the concept of an RSSI, which provides a signal strength measurement.*

Test Your Knowledge

1. You are experiencing problems with a wireless printer that was recently working. How can you verify the IP address?
 - a. Set the **ping** command to **auto** and look for a reply.
 - b. Verify the IP address assigned by entering the command **ipconfig** at the command prompt.
 - c. Remove the cover to the printer to find the MAC address.
 - d. Ping the server
2. What issue is likely to happen if one wireless client is running 802.11b and another is running 802.11g, and both connect to the wireless router at the same time?
 - a. There will be no issues.
 - b. The wireless router will select 802.11g for setting the data transfer rate.
 - c. The wireless router will select 802.11b for setting the data transfer rate.
 - d. The access point will temporarily shut down until one client goes offline.

SUMMARY

This chapter presents an overview of wireless networking, including fundamental concepts and sample networks. The vendors of wireless networking equipment have made their devices easy to integrate into existing networks, but you must understand that the key objective of a network administrator is to provide a fast, reliable, and secure computer network. Carelessly integrating wireless components into a network can easily compromise this objective.

You should understand the following from reading this chapter:

- The operating characteristics of the 802.11 wireless networks
- The purposes of access points, wireless LAN adapters, and wireless bridges
- How to perform a basic site survey on a building
- How to configure a network for user mobility
- How to plan multipoint wireless distribution

Wireless networking technologies have greatly simplified planning and installation. However, they have also brought some complications. For example, any time you are working with RF, there is a chance of unexpected interference and noise. A well-planned RF installation requires a study of all known interference and a search for any possible interference. An RF study should also include signal path studies that enable the user to prepare a well-thought-out plan and allow an excellent prediction of received signal level. The bottom line is to obtain support for conducting an RF study.

QUESTIONS AND PROBLEMS

Section 4-2

1. List two advantages of wireless networking.
User mobility and cost-effectiveness for areas where wiring would be too expensive
2. What are the three areas defined for the IEEE 802.11 standard?
The physical layer, the MAC layer, and wireless management protocols and services
3. What is an ad hoc network?
An ad hoc network is an independent network.
4. What is the purpose of an extended service set?
An ESS uses multiple access points to extend user mobility.

5. What are the four physical layer technologies used in 802.11 wireless networking?

DHSS: direct-sequence spread spectrum

FHSS: frequency-hopping spread spectrum

Infrared

OFDM: orthogonal frequency-division multiplexing

6. Describe the frequency spectrum for the DSSS channels in 802.11b wireless networking.

802.11 DSSS implements 14 channels (each consuming 22MHz) over approximately 90MHz of RF spectrum in the 2.4GHz ISM (industrial, scientific, and medical) band.

7. Define pseudorandom sequence as it applies to FHSS.

Pseudorandom sequence means that the frequency-hopping sequence appears to be random, but it does repeat.

8. What must the FHSS transmitting and receiving units know in order to communicate?

They must know the hopping sequence.

9. What are the frequency range and modulation technique used by 802.11a?

5GHz, OFDM

10. What is the maximum data rate for each of the following?

a. 802.11b

11Mbps

b. 802.11a

54Mbps

c. 802.11g

54Mbps

d. 802.11n

200Mbps+

e. 802.11ac

1Gbps+

f. 802.11ax

10Gbps

11. Define MIMO as it applies to 802.11n.

MIMO (multiple-input multiple-output) uses a technique called space-division multiplexing, in which the data stream is split into multiple parts called spatial streams. The different spatial streams are transmitted using separate antennas.

12. What is the purpose of the power save mode in 802.11n?

With the power save mode, 802.11n uses multiple data paths only when faster data transmission is required, thus saving power.

Section 4-3

13. What is the purpose of an access point?

An access point provides a bridge between a wireless LAN and a wired network.

14. How does an access point know if a wireless data packet is intended for its network?

802.11 wireless LAN devices use an SSID to identify what wireless data traffic is allowed to connect to the network.

15. What is an association, and what is its purpose?

An association is an established wireless connection. An access point uses an association to build a table of users (clients) on the wireless network.

16. Draw a picture of a point-to-point wireless connection.

Refer to Figure 4-9(a)

17. Draw a picture of a point-to-multipoint wireless network.

Refer to Figure 4-9(b)

18. What are the key issues to explore when conducting a site survey for each of the following?

- a. Indoor environment

Electrical power connection point(s)

Wired network connection point(s)

Access point placement

RF coverage area

Bandwidth supported

- b. Outdoor environment

Electrical power for the base access point

Connection back to the home network

Antenna selection

Bandwidth supported

RF coverage

Section 4-4

19. In what frequency band does Bluetooth operate?

The 2.4GHz ISM band

20. How many output power classes does Bluetooth have? List the power level and the operating range for each class.

Bluetooth has four operating classes.

Power Class	Average Output Power	Operating Distance
1	100 mW	~100 meters
2	2.5 mW	~10 meters
3	1 mW	~1 meter
4	0.5 mW	~0.5 meter

21. What is a piconet?

A piconet is an ad hoc network consisting of up to eight Bluetooth devices.

22. What is the purpose of the inquiry procedure in Bluetooth?

A Bluetooth device uses the inquiry procedure to discover other Bluetooth devices or to allow itself to be discovered.

23. What is the purpose of the paging procedure in Bluetooth?

A Bluetooth device uses the paging procedure to establish and synchronize a connection between two networking devices.

24. Define the term backscatter.

Backscatter refers to the reflection of the radio waves striking an RFID tag back to the transmitter source.

25. What are the three parameters that define an RFID system?

Means of powering the tag, frequency of operation, communication protocol

26. Explain how power is provided to a passive RFID tag.

Power is provided by rectifying the RF energy transmitted by the reader that strikes the RF tag antenna.

27. What are three advantages of using an active RFID tag?

Can incorporate wireless Ethernet connectivity, can incorporate location capability, the unit is always turned on

28. What three frequency bands are typically used for RFID tags?

LF: 125/134KHz

HF: 13.56MHz

UHF: 860–960MHz and 2.4GHz

29. What is the WiMAX frequency standard for the United States?
5.8GHz and 2.5GHz
30. Why was OFDM selected for WiMAX?
OFDM was selected for WiMAX because of its improved NLOS characteristics.
31. How does WiMAX differ from Wi-Fi?
Frequency assignments differ and data rates differ, but the main difference is that the WiMAX unit only has to compete once to gain entry to a network.

Section 4-5

32. What type of wireless connection is used to connect a home network to a multipoint distribution site?
Point-to-point
33. Use the Internet to find a source of omnidirectional and directional antennas for each of the following standards:
- a. 802.11b
 - b. 802.11a
 - c. 802.11g
 - d. 802.11n
 - e. 802.11ac
 - f. 802.11ax
34. Prepare a list of three manufacturers for each antenna type. Include cost figures.
There are many sources for wireless network antennas. Expect the students to come up with many possible solutions.

Section 4-6

35. What command can you issue to verify network connectivity in a wireless LAN?
ping
36. True or false: When an association is made between a client and a wireless router, the client with the lowest 802.11 system sets the clock speed.
True
37. True or false: In order to have reliable and good throughput wireless connectivity, the wireless access point and the wireless clients must be compatible and use the same standard.
True

38. What is the purpose of measuring signal strength at the receive location?

The purpose of measuring signal strength at the receive location is to verify that you have good signal level.

39. What happens when wireless cell coverage isn't overlapping?

Weak or dead wireless spots appear, thus creating insufficient wireless coverage.

40. Which of the following are general tips for extending your wireless range? (Select all that apply.)

- a. Make sure the antenna is placed high.
- b. Use a high-gain antenna to help boost the receive signal strength.
- c. Enclose the antenna with brick or concrete.
- d. Place the antenna on the ground.

41. True or false: Microwave ovens can cause interference with Wi-Fi signals.

True

42. The default channel for 802.11b and 802.11g wireless routers is channel 6. If you have interference problems, there may be a wireless router nearby with an SSID using the same channel. You can change the channel to which of the following? (Select all that apply.)

- a. 1
- b. 3
- c. 7
- d. 8
- e. 11

43. What is meant by the term *load issues* regarding wireless access points?

Too many users are connecting to the same access point at the same time.

44. True or false: Once the SSID (service set identifier) has been configured for a computer, it normally does not require reconfiguration. However, when you travel, you should use a PSSID (portable service set identifier) to connect to remote access points.

False

45. What happens when an encryption protocol mismatch occurs?

- a. The SSID has to be reconfigured.
- b. The wireless authentication fails and requires reconfiguration of the client's SSID.
- c. The wireless authentication is not successful, resulting in not being able to connect to the SSID.
- d. The lowest level of encryption is applied.

46. You can avoid security problems when connecting a wireless device to a public hotspot by doing which of the following?
- a. Enabling WPA to secure your data traffic
 - b. Enabling WAP to secure your data traffic
 - c. Disabling WPA
 - d. Disabling WAP
47. Which of the following can introduce signal loss into a wireless connection? (Select all that apply.)
- a. Antenna cable attenuation
 - b. Wrong IP address
 - c. An object blocking the wireless signal
 - d. Radio station broadcast
48. A denial of service (DOS) attack creates client disassociation issues by doing two of the following?
- a. Setting up a continuous ping, thereby taking control of the network
 - b. Replacing the SSID with a PSSID and connecting to non-authenticated access points
 - c. Spoofing a disassociate or deauthenticate message and pretending to be a targeted wireless client
 - d. Downgrading WPA3 to WPA2 encryption
49. An access point typically assigns a 192.168.0.x address to a client. How can you verify the IP address assigned?
- a. By entering the command **config-ip** at the command prompt
 - b. By entering the command **ipconfig** at the command prompt
 - c. By entering the command **configip** at the command prompt
 - d. By pushing the reset button on the WAP
50. When you experience problems with a wireless printer that was recently working, what is the first step you should take?
- a. Restart the printer, your computer, and your wireless router.
 - b. Replace the access point and router and reconfigure both of them.
 - c. Remove the cable connecting the printer and replace it.
 - d. Update the firmware on the wireless router.

Critical Thinking

51. A wireless network receiving site is experiencing occasional loss of signal due to interference. Discuss the steps you would take to correct this problem.

The options for solving this problem vary depending on the location of the network receiving site. If this is an indoor site, an additional access point may be required. For an outdoor site, the antenna might need to be aligned or replaced with a more directional antenna. You also might be able to reduce impacts of RF interference by changing the access point channel. For example, most microwave ovens emit RF signals in the upper third of the 2.4GHz band. You can generally avoid microwave oven interference by tuning nearby access points to channels 1 or 6.

52. Prepare a memo to your supervisor, explaining why it is important to run encryption on your wireless network.

The student should report that it is easy for data to be viewed over an unencrypted wireless network. The student could say something about the fact that sensitive information about personnel or the company is being broadcast to the public if encryption is not used.

53. Your company has a suite in a business complex. Another company in the suite next to you has a wireless 802.11b network with the SSID Company A. You can pick up that company's signal from your suite. Your company would like to put up its own wireless network with two access points. Discuss how you would set up these two access points so that your company can obtain optimal performance.

It is important to determine which of the 802.11b channels the SSID Company A is using. Then you can deploy the wireless access points using different, non-overlapping channels. This will help eliminate interference. Also, it is important to do a site survey within your own suite. You want to place the two wireless access points in such a way that their radio signals provide overlapping coverage for the entire suite and their signal will be minimally reflected by the obstacles within the suite.

Certification Questions

54. True or false: If the signal quality drops from excellent to good, the antenna or access point should be replaced.

False

55. The network administrator is setting up a wireless network. There is a chance of radio interference. How can the network administrator avoid or minimize potential interference problems?

- a. Perform an RF study prior to installation of the wireless network.
- b. Contact all owners of equipment that may cause interference and ask them to use different systems.

- c. Contact the FCC to have the interfering sources shut down.
 - d. All of these answers are correct.
56. Define MIMO relative to 802.11n.
- a. MIMO is a multiplexing technique in which the power is split into multiple parts called spatial currents.
 - b. MIMO is a frequency-division multiplexing technique in which the data stream is split into multiple parts called spectral streams.
 - c. MIMO is an OFDM multiplexing technique in which the digital data is portioned into multiple parts called filtered streams.
 - d. MIMO is a space-division multiplexing technique in which the data stream is split into multiple parts called spatial streams.
57. Which of the following best characterizes CSMA/CA?
- a. It replaces CSMA/CD.
 - b. It provides carrier sense with collision avoidance.
 - c. It provides carrier sense with congestion avoidance.
 - d. It provides congestion sensing with collision avoidance.
58. Which of the following are advantages of 802.11g? (Select all that apply.)
- a. Compatible with 802.11b
 - b. Compatible with 802.11a
 - c. Uses infrared instead of radio
 - d. High speed
59. Which of the following is used in wireless LANs to identify whether a client is to become a member of the wireless network?
- a. SSID
 - b. MAC address
 - c. IP address
 - d. Echo
60. What does the term *last mile* mean in relation to telecommunications?
- a. The distance from an RF transmitter to a receiver in WiMAX
 - b. A measurement of signal coverage for WiMAX and for Wi-Fi
 - c. A term for the last connection prior to linking to the RF transmitter
 - d. The last part of the connection from the telecommunications provider to the customer

61. Which of the following is the best way to extend the radio range of a station's wireless link with one access point?
- a. Add multiple access points
 - b. Add additional wiring
 - c. Add 87BZS encoding
 - d. Add B8ZS encoding
62. Which of the following statements is true?
- a. The Wi-Fi Alliance is an organization that assembles and tests wireless equipment before it is shipped to vendors.
 - b. The Wi-Fi Alliance is an organization that tests and certifies wireless equipment for compliance with the 803.1 standards.
 - c. The Wi-Fi Alliance is an organization that tests and certifies wireless equipment for compliance with the 802.11x standards.
 - d. None of these answers are correct.
63. Which of the following are current wireless networking standards? (Select all that apply.)
- a. 802.12n
 - b. 802.11g
 - c. 803.11g
 - d. 802.11a
 - e. 802.11b
 - f. 802.55a
 - g. 802.11n
 - h. 802.1a
 - i. 802.11ac
 - j. 802.11ax

INDEX

Symbols

? (help) command, 367

Numbers

3DES (Triple Data Encryption Standard), 651

3G wireless standard, 204

4G wireless standard, 204

4G/LTE, 204

5G wireless standard, 204

6to4 prefix, 335

8P8C connectors, 70–71

10BASE2 cabling, 41

10BASE5 cabling, 41

10BASE-FL cabling, 41

10BASE-T cabling, 41

10GBASE-LR cabling, 41

10GBASE-SR cabling, 41

10GBASE-T cabling, 41, 76, 97–98

AXT, 98

full-duplex transmissions, 100

F/UTP, 99

hybrid echo cancellation circuits, 100

IEEE 802.3an-2006, 98

performance, 100–101

PSAACRF, 98, 99

PSANEXT, 98, 99

signal transmission, 100–101

29 CFR 1910.1200 (Hazard Communication), 716

29 CFR 1910.157 (Portable Fire Extinguishers), 712–713

29 CFR 1910.160 (Fixed Extinguishing Systems), 713–714

29 CFR 1910.164 (Fire Detection Systems), 714–715

29 CFR 1910.165 (Employee Alarm Systems), 715–716

29 CFR 1910.36 (Design and Construction Requirements for Exit Routes), 709–710

29 CFR 1910.37 (Maintenance, Safeguards, and Operational Features for Exit Routes), 710

29 CFR 1910.38 (Emergency Action Plans), 710–711

29 CFR 1910.39 (Fire Prevention Plans), 711–712

32-bit CPU architectures, 679

40GBASE-T cabling, 41

64-bit CPU architectures, 679

100BASE-FX cabling, 41

100BASE-SX cabling, 41

100BASE-TX cabling, 41

802.1x (dot1x) wireless standard, 633

802.11 wireless standard, 175–176

ad hoc networks, 176, 177

AP, 177–178

BSS, 176, 177, 178

channel bonding, 179

CSMA/CD, 178

DSSS, 179

ESS, 178

FHSS, 180

frequency channels, 179

hand-offs, 178

hopping sequences, 180

ISM band, 179

MAC layer, 176

OFDM, 180

Open Authentication, 638

PHY layer, 176

pseudorandom numbering sequences, 180

roaming, 178

shared-key authentication, 638

transceivers, 177

transmit power, 180

WMN, 176

802.11a (Wi-Fi 2) wireless standard, 24, 180–181, 183

802.11ac (Wi-Fi 5) wireless standard, 24, 182, 183

802.11ax (Wi-Fi 6) wireless standard, 25, 182, 183

802.11b (Wi-Fi 1) wireless standard, 24, 181, 183

802.11g (Wi-Fi 3) wireless standard, 24, 181, 182, 183

802.11i wireless standard, 183

802.11n (Wi-Fi 4) wireless standard, 24, 181, 182, 183

802.11r wireless standard, 183

802.16a (WiMAX) wireless standard, 200

1000BASE-LX cabling, 41

1000BASE-SX cabling, 41

1000BASE-T cabling, 41

A

A records (Address records), 541–542

AAA (Authentication, Authorization, Accounting) frameworks, 623–624

AAAA records (Quad-A records), 545

A.B.C.D. values, 20–21

absorption, fiber-optic cabling, 136

access

BWA, 199–200

CDMA, 204

- controlling, detection methods, 661–662
 - motion detection*, 662
 - surveillance cameras*, 662
- controlling, physical security, 659, 660–661
 - access control vestibules (mantraps)*, 661
 - badge readers*, 661
 - biometric scanners*, 661
 - locking cabinets*, 661
 - locking racks*, 661
- door access, 717
- home access, home networks, 31
- HSPA+204
- NAC, 624
- network access management, 623–624
- public access, home networks, 31
- RAS, 647
- RBAC, 623
- remote access security, 642
 - analog modems*, 643–644
 - cable modems*, 644
 - RAS*, 647
 - xDSL modems*, 644–646
- routers, 626–628
- TACACS+624
- WPA, 215, 639
- WPA2, 639–640
- WPA3, 640
- access control vestibules (mantraps), 661**
- access points (AP), 177–178, 186–187, 189–190**
 - evil twin attacks, 598
 - home networks, 28
 - troubleshooting, 213
- access/edge layer, LAN, 269**
- access-list permit ip any any command, 617**
- accounting, AAA framework, 623–624**
- ACK (Acknowledgement) packets, 297**
- ACL (Access Control Lists), 617–618**
- ACR (Attenuation to Crosstalk Ratios), 93, 95**
 - PSAACRF, 98, 99
 - PSACR, 93, 95, 96
- active/active disaster recovery architectures, 731**
- active/passive disaster recovery architectures, 731**
- active RFID tags, 202**
- ad hoc networks, 176, 177**
- adapter addresses. See MAC addresses**
- adaptive cut-through mode, switches, 247**

addresses

- adapter addresses. *See* MAC addresses
- anycast addresses, 335
- broadcast addresses, subnetting, 322
- class network addresses, 467
- classful addresses, 317, 467
- DAD, 337
- Ethernet addresses. *See* MAC addresses
- gateway addresses, 265, 326–327, 359–361
- HA, 302
- hardware addresses. *See* MAC addresses
- IPv4 addressing, 20, 312–313
 - 6to4 prefix*, 335
 - A.B.C.D. values*, 20–21
 - APIPA*, 532, 533
 - ARIN*, 315
 - assigning*, 315, 529–530
 - class network addresses*, 467
 - classes*, 313
 - classful addresses*, 317
 - decimal/binary octets*, 314
 - default gateway addresses*, 359–361
 - dual stacks*, 336
 - host IP addresses*, 315
 - host numbers*, 21
 - lease time*, 532
 - managing with DHCP*, 531–537
 - network/host bits*, 314–315
 - network numbers*, 21, 482
 - next hop addresses*, 362
 - non-Internet-routable IP addresses*, 316
 - Office LAN*, 40
 - overloading*, 35
 - private IP addresses*, 21–22, 316
 - public IP addresses*, 22
 - RIR*, 315
 - structure of*, 313
 - switches*, 245
 - TCP/IP*, 21–22
 - transitioning to IPv6*, 335–337
 - wildcard bits*, 482–483
- IPv6 addressing, 333–335
 - 6to4 prefix*, 335
 - anycast addresses*, 335
 - CIDR*, 337–338
 - DAD*, 337

- defined, 333*
- dual stacks, 336*
- interface (host) identifiers, 335*
- IPng, 333*
- link-local addresses, 335, 336–337*
- multicast addresses, 335*
- routing, 499*
- routing, BGP, 501–502*
- routing, EIGRP, 501*
- routing, OSPF, 500–501*
- routing, RIP, 499–500*
- routing, static, 499*
- SLAAC, 336–337*
- transitioning to, 335–337*
- unicast addresses, 335*
- link-local addresses, 335, 336–337
- logical addresses, 249
- MAC addresses
 - CAM, 246*
 - defined, 18*
 - destination MAC addresses and sources, 17*
 - filtering, 33*
 - length of, 18*
 - NIC, 18*
 - Office LAN, 40*
 - OUI, 18*
 - sampling of, 18*
 - spoofing attacks, 635*
 - sticky command option, 634*
- multicast addresses, 303, 335
- NAT, 34
 - defined, 34*
 - private IP addresses, 34–35*
 - public IP addresses, 35*
- NET addresses, 479
- network addresses, 249, 322
- next hop addresses, 362
- PA, 301
- physical addresses. *See* MAC addresses
- secure addresses, switches, 243
- unicast addresses, 335, 533
- administrative distance, 461**
- administratively down, 390**
- ADSL (Asymmetric DSL), 645–646**
- advertising, routes, 466**
- AES (Advanced Encryption Standard), 640**
- aging time, 244**
- AH (Authentication Headers), 651**
- air interface (communications) portal, RFID tags, 203**
- alarms, CSU/DSU, 272**
- analog modems**
 - asymmetric operations, 643
 - security, 643–644
 - V.44/V.34 modem standard, 643
 - V.92/V.90 modem standard, 643
- analyzing network traffic, 552–565**
- ANDing, subnet masks, 361–362**
- ANT+ wireless technology, 183**
- antennas**
 - dish (parabolic reflector) antennas, 209
 - EIRP, 210
 - multipoint distributions, 209–211
 - omnidirectional antennas, 208–209
 - placement of, point-to-multipoint WLAN case study, 207
 - ranges (wireless), extending, 214
 - remote installations, 211
 - RF site surveys, 209–211
 - selecting, 208–209
 - site surveys, 207
 - spatial diversity, 186
 - Yagi antennas, 209
- antivirus/anti-malware software, 610–611**
- anycast addresses, 335**
- AP (Access Points), 177–178, 186–187, 189–190**
 - evil twin attacks, 598
 - home networks, 28
 - troubleshooting, 213
- APC connectors, 64, 146**
- APIPA (Automatic Private IP Addressing), 532, 533**
- appearance, home networks, 31**
- Application layer**
 - OSI model, 13, 14
 - TCP/IP, 294, 295–296
- applications (common) and port numbers, 295–296**
- Area 0, OSPF, 482**
- areas, OSPF, 477**
- ARIN (American Registry for Internet Numbers), 315, 529**
- ARP (Address Resolution Protocol), 301–303, 563**
 - bridges, 233–235
 - caches, 233–235
 - caches, poisoning, 598
 - DAI, 635

- expired entries, 235
- replies, 563–564
- spoofing attacks, 635
- ARPANET (Advanced Research Projects Agency Network), 292**
- assembling Office LAN, 38–39**
 - cabling, 40–43
 - client/server networks, 42–45
 - diagramming networks, 39–40
 - IP addressing, 40
 - MAC addresses, 40
 - network device connections, 40–43
 - peer-to-peer networks, 42, 43
- asset disposal, 662**
- asset/inventory management, 728**
- assigning**
 - IP addressing, 529–530
 - IPv4 addresses, 315
 - protocols, 529
- associations, LAN interconnections, 233**
- associations, wireless connections, 186–187, 193**
- asymmetric operations, modems, 643**
- attacks, network security**
 - ARP cache poisoning, 598
 - botnets, 608
 - brute-force attacks, 596
 - buffer overflow attacks, 599–600
 - coordinated DDoS attacks, 608
 - DDoS attacks, 608–609
 - deauthentication/disassociation attacks, 608
 - dictionary attacks, 596
 - directed broadcasts, 607
 - DoS attacks, 606–609
 - evil twin attacks, 598
 - intrusion attacks, 594–604
 - logic bombs, 604
 - malware, 602–604, 610–611
 - on-path attacks (man-in-the-middle attacks), 598
 - packet sniffing attacks, 597–599
 - password cracking attacks, 596–597
 - PDoS attacks, 607
 - ransomware attacks, 604
 - reflective/amplified DoS attacks, 608
 - session hijacking, 599
 - social engineering attacks, 595–596
 - software vulnerabilities, 599–604
 - spoofing attacks, 607, 635

- viruses, 602–603, 610–611
- VLAN hopping, 599
- worms, 603
- zero-day attacks, 604
- attenuation (insertion loss), 92, 93–94**
 - ACR, 93, 95
 - fiber-optic cabling, 127, 136–137, 142
 - PSAACRF, 98, 99
 - PSACR, 93, 95, 96
- audits, IT, 728**
- AUP (Acceptable Use Policies), 725**
- authentication**
 - AAA framework, 623–624
 - AH, 651
 - CCMP, 639–640
 - CHAP, 649, 650
 - deauthentication/disassociation attacks, 215
 - EAP, 640, 650
 - Kerberos, 623
 - LEAP, 640
 - MD5 hashing algorithm, 649, 650
 - Open Authentication, 638
 - PAP, 649–650
 - RADIUS, 624, 640
 - SHA, 649, 650
 - shared-key authentication, 638
- authorization, AAA framework, 623–624**
- auto-negotiation, 383–386**
- AS (Autonomous Systems), 529**
- auxiliary input, routers, 250**
- AXT (Alien Crosstalk), 98**

B

- backbone**
- backbones**
 - cabling, 67, 155
 - defined, 477
- backscatter, 200**
- backups, 729–730**
- badge readers, 661**
- balanced mode, 74–75**
- bandwidth**
 - fiber-optic cabling, 126
 - metrics, 461
 - multilevel encoding, 100

BD (Building Distribution) fiber, optical networking, 151–154

beacons, 638

beamforming, 182

best practices

- asset/inventory management, 728
- backups, 729–730
- configuration standards, 727–728
- documentation, 727
- HA, 730–731
- IT audits, 728
- role separation, 728

BGP (Border Gateway Protocol), 496–498, 501–502

BiDi (Bidirectional) transceivers, 154

binary numbers

- binary-to-decimal conversions, 306–307
- decimal-to-binary conversions, 307–309
- IPv4 addressing, 314

biometric scanners, 661, 717

BLE (Bluetooth Low Energy) technology, 197

blocked TCP/UDP ports, troubleshooting, 573

blocking state, STP, 423

Bluejacking, 641

Bluesnarfing, 641

Bluetooth

- BLE technology, 197
- enabling connections, 198–199
- inquiry procedures, 197
- output power classes, 197
- paging procedures, 197
- piconets, 197–198
- security, 641

BNC connectors, 64

bonding, channel (Ethernet), 179

BOOTP (Bootstrap Protocol), 531

botnets, 608

bottlenecking (network congestion), 76, 252

bottom-to-top (bottom-up) troubleshooting approach, 569

BPDU (Bridge Protocol Data Units), 422–423

BPDU Filter, 636

BPDU Guard, 635–636

branching devices, 142

bridges

- advantages/disadvantages of, 236
- ARP caches, 233–235
- associations, 233
- broadcasts, 233
- defined, 232
- MAC addresses, 232–234
- multiport bridges. *See* layer 2 switches
- ports, 232–233
- translation bridges, 235
- transparent bridges, 235
- wireless bridges, 187–189, 236

broadband modems/gateways, 28

broadcast addresses, subnetting, 322

broadcast domains, 246, 358

broadcasts

- bridges, 233
- broadcast storms, 233
- defined, 9
- directed broadcasts, 607
- SSID broadcasts, turning off, 33

brute-force attacks, 596

BSS (Basic Service Sets), 176, 177, 178

buffer overflow attacks, 599–600

buffering/queuing, 252

building distributions, optical networking, 151–154

building entrances, structured cabling, 66–67

bus topologies, 8–9

business policies/procedures, 723

- asset/inventory management, 728
- AUP, 725
- backups, 730
- best practices, documentation, 727
- configuration standards, 727–728
- continuity/recovery policies/procedures, 729
 - MTBF*, 729
 - MTTF*, 729
 - MTTR*, 729
- HA, 730–731
- incident response policies, 725
- IT audits, 728
- MLA, 724
- MOU, 723–724
- MSA, 724
- NDA, 725
- onboarding/offboarding policies, 727
- password policies, 726
- privileged user agreements, 726
- role separation, 728
- SLA, 724

SOP, 726–727

SOW, 725

business policies/procedures. *See also* rules/regulations

BWA (Broadband Wireless Access), 199–200

BYOD (Bring Your Own Device), 568

C

cabinets, locking, 661

cable modems

home networks, 28, 29

security, 644

cabling

8P8C connectors, 70–71

10BASE2 cabling, 41

10BASE5 cabling, 41

10BASE-FL cabling, 41

10BASE-T cabling, 41

10GBASE-LR cabling, 41

10GBASE-SR cabling, 41

10GBASE-T cabling, 41, 76, 97–98

AXT, 98

full-duplex transmissions, 100

F/UTP, 99

hybrid echo cancellation circuits, 100

IEEE 802.3an-2006, 98

performance, 100–101

PSAACRF, 98, 99

PSANEXT, 98, 99

signal transmission, 100–101

40GBASE-T cabling, 41

100BASE-FX cabling, 41

100BASE-SX cabling, 41

100BASE-TX cabling, 41

1000BASE-LX cabling, 41

1000BASE-SX cabling, 41

1000BASE-T cabling, 41

attenuation (insertion loss), 92, 93–94

backbone cabling, 67

balanced mode, 74–75

CAT5, patch cabling, CAT5, assembling, 87–90

CAT5e, test examples, 104–109

CAT6 cabling, 40

certification, 93–96

channel specifications, 93–96

coaxial cabling, 64

console cabling, 250, 255

crossover cabling, 41–42, 83

crosstalk, 94

ELFEXT, 93, 95

Ethernet LAN cabling, numerics, 41

Fast Ethernet, 76

fiber-optic cabling

absorption, 136

advantages of, 126–127

APC connectors, 146

attenuation (insertion loss), 127, 136–137

attenuators, 142

backbones, 155

bandwidth, 126

BD fiber, 151–154

branching devices, 142

building distributions, 151–154

campus networks, 154–157

chromatic dispersion, 137–138

cladding, 130

color-coding fiber, 156

components of, 126, 141–142

connectorization, 145–146

cores, 130

corrosion, 127

costs, 127

crosstalk, 127

CWDM, 142

detectors, 143–145

DFB lasers, 141

diplexers, 154

dispersion, 137–139

dispersion compensation, 139

dispersion shifted fibers, 138–139

DL, 141

DWDM, 130, 141

electrostatic interference, 126

Ethernet, 157

events, troubleshooting, 162

FC connectors, 145–146

fiber, 142

fiber Bragg grating, 139

fiber cross-connects, 151

fiber selection, 132–133

fiber-to-the-home/business, 130

FTTB, 149

FTTC, 149
FTTD, 149
FTTH, 149
fusion splicing, 144
GBIC, 152–153
glass, 142
graded-index fiber, 132, 133–134
IC fibers, 152
IDC, 152–153
index-matching gel, 144
IR (Infrared) radiation, 126
isolators, 142
LC connectors, 145–146
LED, 141
light pipes, 142
link budgets, 157–158
logical fiber maps, 154, 155
mechanical splicing, 144–145
microbending, 136–137
mm fibers, 155
modal dispersion, 137–138
mode field diameters, 134–135
MT-RJ connectors, 145–146
multimode fiber, 130, 132
numerical apertures, 131
optical connectors, 126
optical Ethernet, 149–150
optical networking, defined, 148–151
optical spectrum, 130–131
optical-line amplifiers, 143
OTDR, 162–163
photosensitive detectors, 126
physical fiber maps, 154, 156
polarization mode dispersion, 137, 139
pulse dispersions, 132–133
refraction of light, 129
refractive indexes, 129
RSL, 142
safety, 127, 160–161
SC connectors, 145–146
scattering, 136
security, 127
SFP, 152–153
SFP+ 153–154
“shooting the fiber”, 162
single-mode fibers, 130, 134–135
sm fibers, 155
splitters, 142
ST connectors, 145–146
step-index fiber, 133
strands, 131–132
transceivers, 154
transmission strands, 126
troubleshooting, 162–163
tunable lasers, 141–142
“two-deep” rule, 152–153
unconnected fibers, 146
UPC connectors, 146
VCSEL, 141
VFL, 162
WDM, 130, 143
X2, 153–154
XENPAK, 153–154
XFP, 153–154
XPAK, 153–154
zero dispersion wavelengths, 138–139
 full channels, 92
 full-duplex cabling, 76
 F/UTP, 99
 Gigabit Ethernet, 76
 HC, 68, 69
 horizontal cabling, 67, 69–73, 83–87
 hybrid echo cancellation circuits, 100
 IC, 68, 69
 links, 92
 managing, 67
 manufacturer’s specifications, 102–104
 MC, 68, 69
 multilevel encoding, 100
 NEXT, 92, 93, 94–95
 patch cabling, 71–72, 82
 performance, 110
 physical layer cabling, 64
 10 Gigabit Ethernet over Copper, 97–101
 APC connectors, 64
 BNC connectors, 64
 cable testing/certification, 92–96
 connectors, 64
 fiber couplers, 64
 structured cabling, 66–73
 troubleshooting, 102–110
 twisted-pair cabling, 74–77

- twisted-pair cabling, terminating, 78–90*
- UPC connectors, 64*
- UTP couplers, 64*
- PSELFEXT, 93, 95, 96
- PSNEXT, 93, 94
- RJ-45 connectors, 40, 70–71, 75
- rollover cabling, 255–256
- STP cabling, 76–77
- straight-through cabling, 82, 87–90
- structured cabling
 - backbone cabling, 67*
 - building entrances, 66–67*
 - ER, 67*
 - HC, 68, 69*
 - horizontal cabling, 67, 69–73*
 - IC, 68, 69*
 - MC, 68, 69*
 - STP cabling, 76–77*
 - TCO, 67*
 - telecommunications closets, 67, 69–70*
 - TIA/EIA 568-A cabling standard, 66*
 - TIA/EIA 568-B cabling standard, 66*
 - TIA/EIA 569B cabling standard, 66–67*
 - UTP cabling, 74–76*
 - WO, 68*
 - work areas, 67*
- T568A wiring standard
 - color maps, 78–80*
 - defined, 78*
 - pinouts, 79*
- T568B wiring standard
 - color maps, 78–80*
 - defined, 78*
 - pinouts, 79*
- TCO, 67
- termination, 70
- testing, 92–93
 - ACR, 93, 95*
 - attenuation (insertion loss), 92, 93–94*
 - channel specifications, 93–96*
 - delay skew, 93, 96*
 - ELFEXT, 93, 95*
 - near-end testing, 94*
 - NEXT, 92, 93, 94–95*
 - propagation delay, 93, 96*
 - PSACR, 93, 95, 96*
 - PSELFEXT, 93, 95, 96*
 - PSNEXT, 93, 94*
- Thin/Net cabling, bus topologies, 8
- troubleshooting, 102
 - connectivity, 110*
 - DTX-1800 certification reports, 103, 104*
 - failures to meet manufacturer specifications, 102–104*
 - multimeters, 110*
 - performance, 110*
 - stretching, 102*
- twisted-pair cabling
 - ELTCTL, 99*
 - F/UTP, 99*
 - LCL, 99*
 - return loss, 93, 95–96*
 - STP cabling, 76–77*
 - TCL, 99*
 - TCTL, 99*
 - terminating, 78–80*
 - UTP cabling, 74–76*
- UTP cabling, 76
 - CAT3, 75, 76*
 - CAT5, 74, 75, 76*
 - CAT5, patch cabling, 87–90*
 - CAT5, straight-through cabling, 87–90*
 - CAT5e, 74, 75, 76, 79–82*
 - CAT5e, patch cabling, 87–90*
 - CAT5e, straight-through cabling, 87–90*
 - CAT5e, test examples, 104–109*
 - CAT6, 74, 75, 76, 79–82, 83–87*
 - CAT6a, 75, 76*
 - CAT7, 74, 75, 79–82*
 - CAT7a, 75*
 - CAT8, 74, 75, 79–82*
- UTP, F/UTP, 99
- wiremaps, 82
- WLAN, troubleshooting, 215
- WO, 68
 - work areas, 67*
- cache poisoning, ARP, 598**
- caches, virtualization, 679**
- CAM (Content-Addressable Memory), 246**
- cameras**
 - IP security cameras, 662
 - surveillance, 662

campus networks

- backbones, 477
- defined, 230
- hierarchical topologies, 69
- optical networking, 154–157

CAN (Campus Area Networks), 5**captive portals, home networks, 32****Carrier Ethernet, 273–274****CAT3**

- twisted-pair cabling, 75
- UTP cabling, 76

CAT5

- patch cabling, 87–90
- straight-through cabling, 87–90
- UTP cabling, 74, 75, 76

CAT5e

- patch cabling, 87–90
- straight-through cabling, 87–90
- test examples, 104–109
- UTP cabling, 74, 75, 76, 79–82

CAT6

- cabling, 40
- horizontal cabling, terminating, 83–87
- UTP cabling, 74, 75, 76, 79–82

CAT6a, UTP cabling, 75, 76**CAT7**

- STP cabling, 76–77
- UTP cabling, 74, 75, 79–82

CAT7a, UTP cabling, 75**CAT8**

- STP cabling, 76–77
- twisted-pair cabling, 75, 79–82
- UTP cabling, 74

CBS (Committed Burst Size), 276**CCMP (Cipher Mode with Cipher Block Chaining Message Authentication Code Protocol), 639–640****ccTLD, 528****CDMA (Code-Division Multiple Access), 204****cellular (mobile) communications, 204**

- 3G wireless standard, 204
- 4G wireless standard, 204
- 5G wireless standard, 204
- CDMA, 204
- EDGE, 204
- geofencing, 204

HSPA+204

LTE/4G, 204

NFC, 204

certification

- cabling, 93–96
- DTX-1800 certification reports, 103, 104

CFR (Code of Federal Regulations), 709**change management policies, 624****changing**

- factory passwords, 33
- SSID, 33

channel bonding, 179**channel specifications, cabling, 93–96****channel utilization (WLAN), troubleshooting, 214–215****CHAP (Challenge Handshake Authentication Protocol), 649, 650****check sequences, frames, 17****chromatic dispersion, 137–138****CIDR (Classless Interdomain Routing), 329**

- blocks, 330–331
- IPv6 addressing, 337–338
- notation, 329
- subnet mask conversions, 329–330

CIR (Committed Information Rates), 276**Cisco, remote client VPN configurations, 653–657****cladding, fiber-optic cabling, 130****class network addresses, 467****classes, IPv4 addressing, 313****classful addresses, 317, 467****client/server networks, 42–45****client-to-site VPN, 648****cloud computing, 693–694**

- advantages/disadvantages of, 695–696
- cloud services, 692–693
- community clouds, 696
- CSP, 696
- DaaS, 695
- defined, 692
- elasticity, 696
- email, 693
- hybrid clouds, 696
- IaaS, 694
- infrastructures, 696–697
- multitenancy, 695, 696
- outsourcing, 692
- PaaS, 695

- private clouds, 696
- public clouds, 696
- SaaS, 695
- scalability, 695–696
- SDN, 696–697
- security, 697
- SLA, 693
- cloud sites, disaster recovery, 731**
- CM-54 Beasley-Networking Essentials, 6e, 9780137455928, 5**
- CNA (Cisco Network Assistant), switches, 242–243**
- CNAME records (Canonical Name Records), 542–543, 693**
- coaxial cabling, 64**
- cold sites, disaster recovery, 731**
- cold/hot’ aisles, 73**
- collision domains, isolating, 246**
- collisions, switches, 433**
- color maps, T568A/T568B wiring standards, 78–80**
- color-coding, fiber-optic cabling, 156**
- command prompt, Windows 10, 18**
- common applications and port numbers, 295–296**
- communications (air interface) portal, RFID tags, 203**
- community clouds, 696**
- compatibility (wireless), troubleshooting, 213**
- computer forensics, 621**
- configuration standards, 727–728**
- configure terminal (conf t) command, 374, 411**
- configuring (setting up)**
 - BGP, 496–498
 - computers for LAN operation, 44
 - EIGRP, 488–494
 - FastEthernet interfaces, 376–377
 - firewalls, 611–617
 - interfaces, auto-negotiation, 383–386
 - IP addressing, switches, 245
 - OSPF, 481–485
 - PuTTY software, 256–259
 - routers
 - Privileged EXEC mode (Router#), 380–381*
 - User EXEC mode (Router>), 369–371*
 - SLAAC, 336–337
 - SNMP, 547–551
 - static routing, 454–458
 - static VLAN, 414–418
 - switches, 410, 419–420
 - configure terminal (conf t) command, 411*
 - enable secret command, 412*
 - hostname command, 411–412*
 - line console passwords, 412–414*
 - privileged mode, 411, 412*
 - static VLAN configurations, 414–418*
 - switch# prompt, 412*
 - switch(config)# prompt, 411, 412*
 - switch(config-line)# prompt, 413*
 - VLAN subinterfaces, 418–419*
- virtualization, 682–690
- WLAN, 185–195, 206–211
- congestion (bottlenecking), networks, 76, 252**
- connection-oriented protocols, 297**
- connectivity**
 - networks
 - home networks, 32*
 - verifying with ping command, 240–241*
 - ZTerm serial communications software, 259–261*
 - troubleshooting, 110
- connectorization, fiber-optic cabling, 145–146**
- connectors**
 - 8P8C connectors, 70–71
 - APC connectors, 64
 - BNC connectors, 64
 - DB-9 connectors, 254–255
 - DB-25 connectors, 254, 255
 - fiber couplers, 64
 - RJ-45 connectors, 70–71, 75, 255
 - UPC connectors, 64
 - UTP couplers, 64
- console cabling, 255**
- console input/cabling, 250**
- console ports, routers**
 - console cabling, 255
 - DB-9 connectors, 254–255
 - DB-25 connectors, 254, 255
 - PuTTY software, 256–259
 - RJ-45 connectors, 255
 - rollover cabling, 255–256
 - RS-232 serial communications ports, 254, 255
 - serial interfaces, 256
 - ZTerm serial communications software, 259–261
- content filters, 620**

- contiguous networks, 467**
- continuity/recovery policies/procedures, 729**
 - MTBF, 729
 - MTTF, 729
 - MTTR, 729
- controllers, wireless, 189**
- controlling access, physical security, 659, 660–661**
 - access control vestibules (mantraps), 661
 - badge readers, 661
 - biometric scanners, 661
 - locking cabinets, 661
 - locking racks, 661
- convergence, dynamic routing protocols, 460**
- conversion loss, cabling**
 - ELTCTL, 99
 - LCL, 99
 - TCL, 99
 - TCTL, 99
- converting numbers**
 - binary-to-decimal conversions, 306–307
 - decimal-to-binary conversions, 307–309
 - hexadecimal numbers, 309–311
- coordinated DDoS attacks, 608**
- copper, 10GBASE-T cabling, 97–98**
 - AXT, 98
 - full-duplex transmissions, 100
 - F/UTP, 99
 - hybrid echo cancellation circuits, 100
 - IEEE 802.3an-2006, 98
 - performance, 100–101
 - PSAACRF, 98, 99
 - PSANEXT, 98, 99
 - signal transmission, 100–101
- copy running-configuration startup-configuration (copy run start) command, 457**
- core layer, LAN, 268**
- cores**
 - fiber-optic cabling, 130
 - virtualization, 679
- corrosion, fiber-optic cabling, 127**
- costs**
 - fiber-optic cabling, 127
 - home networks, 30
 - metrics, 461
- country domains, 539**

- couplers**
 - fiber couplers, 64
 - UTP couplers, 64
- CRC (Cyclic Redundancy Checksum) errors, 432**
- cross-connects**
 - defined, 68, 69
 - fiber cross-connects, 151
 - HC, 68, 69
 - IC, 68, 69
 - MC, 68, 69
 - WO, 68
- crossover cabling, 41–42, 83**
- crosstalk, 94**
 - ACR, 93, 95
 - AXT, 98
 - fiber-optic cabling, 127
 - PSAACRF, 98, 99
 - PSACR, 93, 95, 96
- crypto key generate rsa command, 628**
- CSMA/CD (Carrier-Sense Multiple Access/Collision Domains), 16, 178**
- CSP (Cloud Service Providers), 696**
- CSU/DSU (Channel Service Units/Data Service Units), 272**
- cut-through mode, switches, 247**
- CWDM (Coarse Wavelength Division Multiplexing), 142**

D

- DaaS (Infrastructure as a Service), 695**
- DAD (Duplicate Address Detection), 337**
- DAI (Dynamic ARP Inspection), 635**
- DARPA (Defense Advanced Research Projects Agency), 292**
- data, frames, 17**
- data centers**
 - architectures, 269
 - “hot/cold” aisles, 73
 - racks
 - diagrams, 72
 - locks, 73
- data channels, interconnecting LAN, 270–271**
- Data link layer, OSI model, 13**
- data packets**
 - ACK packets, 297
 - ARP packets, 302–303

- DHCP packets, 534
- error thresholds, 247
- filtering, 618
- FTP data packets, 566–567
- hello packets, 477
- ICMP source-quench packets, 302
- IGMP packets, 303–304
- keepalive packets, 388
- shaping, 253, 620
- sniffing attacks, 597–599
- SYN ACK packets, 297
- SYN packets, 297
- TCP packets
 - terminating connections*, 299–300
 - transmitting*, 298
- UDP packet transfers, 300–301
- WEP, 638–639
- wire speed routing, 247
- data rates**
 - DS-0 to DS-3, 270
 - E1 to E3, 271
 - T1 to T3, 270
- data speeds, home networks, 30**
- data transmissions, long hauls, 134**
- DB-9 connectors, 254–255**
- DB-25 connectors, 254, 255**
- DDoS (Distributed DoS) attacks, 608–609**
- deauthentication/disassociation attacks, 215, 608**
- decimal numbers**
 - binary-to-decimal conversions, 306–307
 - decimal-to-binary conversions, 307–309
 - IPv4 addressing, 314
- default gateways**
 - addresses, 359–361
 - static routing, 448
- delay metrics, 461**
- delay, propagation, 93, 96**
- delay skew, 93, 96**
- demarcation, lines of, 271**
- DES (Data Encryption Standard), 651**
- Design and Construction Requirements for Exit Routes (29 CFR 1910.36), 709–710**
- desktops, virtual vs remote, 695**
- destination MAC addresses and sources, defined, 17**
- detection methods, 661–662**
 - motion detection, 662
 - surveillance cameras, 662
- detectors, fiber-optic cabling, 143–145**
- deterministic networks, 7**
- device density, 189**
- DFB (Distributed Feedback) lasers, 141**
- DHCP (Dynamic Host Configuration Protocol)**
 - data packets, 534
 - deploying, 535–537
 - DHCP ACK, 532
 - DHCP Discover, 532
 - DHCP Offer, 532
 - DHCP Request, 532
 - IP address management, 531–537
 - snooping, 572
 - troubleshooting, 216, 571–572
- diagramming networks, 39–40**
- dialup modems, 644**
- dictionary attacks, 596**
- differential backups, 730**
- Diffie-Hellman key exchange, 651**
- dig command, 541**
- diplexers, 154**
- directed broadcasts, 607**
- disabled state, STP, 423**
- disassociation/deauthentication attacks, 215, 608**
- disaster recovery**
 - active/active architectures, 731
 - active/passive architectures, 731
 - cloud sites, 731
 - cold sites, 731
 - hot sites, 731
 - policies/procedures, 729
 - MTBF*, 729
 - MTTF*, 729
 - MTTR*, 729
 - RPO, 732
 - RTO, 732
 - sites, 731
 - virtualization, 681
 - warm sites, 731
- dish (parabolic reflector) antennas, 209**
- dispersion, fiber-optic cabling, 137–138**
- dispersion compensation, 139**
- dispersion shifted fibers, 138–139**

- disposal of assets, 662**
- distance vector protocols, 463**
 - hop count metrics, 463–464
 - RIP, 465
 - configuring, 466–468*
 - IPv6, 499–500*
 - link state protocols and, 477*
 - [rip_tag] tags, 500*
 - route configuration, 468–473*
 - sh run command, 471–472*
 - show ip protocol (sh ip protocol) command, 469–471*
 - RIPv2, 474–475
 - configuring, 466–468*
 - route configuration, 473–474*
 - routing loops, 465
- distance, WLAN, 189–190**
- distribution/aggregation layer, LAN, 269**
- divide-and-conquer troubleshooting approach, 569**
- DKIM (Domain Keys Identified Mail), 544**
- DL (Diode Lasers), 141**
- DMT (Discreet Multitone) modulation, 645–646**
- DMZ (Demilitarized Zones), 618**
- DNS (Domain Name Systems), 539**
 - dig command, 541
 - forward DNS lookups, 539
 - nslookup command, 541
 - reverse DNS lookups, 539
 - root DNS servers, 539–540
 - RR, 541–546
 - tree hierarchies, 539–540
- DOCSIS (Data Over Cable Service Interface Specification), 644**
- documentation**
 - AUP, 725
 - best practices, 727
 - change management policies, 624
 - incident response policies, 725
 - MLA, 724
 - MOU, 723–724
 - MSA, 724
 - MSDS, 716
 - NDA, 725
 - onboarding/offboarding policies, 727
 - password policies, 726
 - privileged user agreements, 726
 - SDS, 716
 - security, 624
 - SLA, 724
 - SOP, 726–727
 - SOW, 725
- domain names, managing, 528**
- domain registrars, 530**
- dongles, 682**
- door access, 717**
- doorbells, smart, 663**
- DoS (Denial-of-Service) attacks, 606–609**
- dot1x (802.1x) wireless standard, 633**
- down, administratively, 390**
- DS (Digital Signals), 270**
- DS-0 to DS-3 data rates, 270**
- DSL (Digital Subscriber Lines)**
 - ADSL, 645–646
 - modems, home networks, 29–30
 - services, 645
 - xDSL
 - modems, 644–646*
 - services, 645*
- DSSS (Direct-Sequence Spread Spectrum), 179**
- DTLS (Datagram Transport Layer Security) protocol, 598**
- DTX-1800 certification reports, 103, 104**
- dual stacks, 336**
- duplex operations. See building distributions**
- DWDM (Dense Wavelength Division Multiplexing), 130, 141**
- dynamic (private) ports, 295**
- dynamic assignments, 243**
- dynamic routing protocols, 460, 461**
 - convergence, 460
 - load balancing, 460
 - metrics, 460, 461
 - path determination, 460
- dynamic VLAN, 408**

E

- E1 to E3 data rates, 271**
- EAP (Emergency Action Plans), 710–711**
- EAP (Encryption Authentication Protocol), 640, 650**
- ease of implementation, home networks, 31**
- EBS (Excess Burst Size), 276**
- echo requests, 564–565**

EDGE (Enhanced Data GSM Evolution), 204
education records, FERPA, 719
EF (Entrance Facilities), structured cabling, 67
EIA (Electronic Industries Alliance)
 defined, 66
 TIA/EIA 568-A cabling standard, 66
 TIA/EIA 568-B cabling standard, 66
 TIA/EIA 569B cabling standard, 66–67
EIGRP (Enhanced Interior Gateway Routing Protocol), 487–494, 501
EIR (Excess Information Rates), 276
EIRP (Effective Isotope Radiated Power), 210
E-LAN (Ethernet LAN) service, 275
elasticity, cloud computing, 696
electromagnetic wavelength spectrum, 131
electrostatic interference, fiber-optic cabling, 126
ELFEXT (Equal-Level FEXT), 93, 95
E-Line (Ethernet Service Line), 274, 275
ELTCTL (Equal Loss Transverse Conversion Transfer Loss), 99
email
 cloud computing, 693
 CNAME records, 693
 MX records, 693
Emergency Action Plans (29 CFR 1910.38), 710–711
Employee Alarm Systems (29 CFR 1910.165), 715–716
enable command, routers, privileged mode, 373
enable secret command, 375, 412
encoding, multilevel, 100
encryption
 3DES, 651
 AES, 640
 DES, 651
 home networks, 33
 Type 5 encryption algorithm, 627
 Type 7 encryption algorithm, 627
 wireless networks (Wi-Fi), 33
enterprise networks, 5, 262
enterprise storage
 NAS, 700
 SAN, 698–699
ER (Equipment Rooms), structured cabling, 67
error thresholds, 247
ESP (Encapsulating Security Protocols), 651
ESS (Extended Service Sets), 178

Ethernet
 10GBASE-T cabling, 97–98
 AXT, 98
 full-duplex transmissions, 100
 F/UTP, 99
 hybrid echo cancellation circuits, 100
 IEEE 802.3an-2006, 98
 performance, 100–101
 PSAACRF, 98, 99
 PSANEXT, 98, 99
 signal transmission, 100–101
 bonding, 179
 Carrier Ethernet, 273–274
 Ethernet Service Definition, 274
 EVC, 274
 Fast Ethernet, 76
 FastEthernet ports, 250
 FCoE, 699
 giants, 433
 Gigabit Ethernet, 76
 MEF, 274
 MOE, 273–274
 optical Ethernet, 149–150
 optical networking, 157
 PoE, 425–428
 PoE+427
 PoE++428
 runts, 433
 service attributes, 276–277
Ethernet addresses. See MAC addresses
Ethernet jumbo frames, preambles, 17
Ethernet LAN, 16
 cabling, numerics, 41
 CSMA/CD, 16
 frames, 17
 check sequences, 17
 components of (overview), 17
 data, 17
 data structure of, 17
 destination MAC addresses and sources, 17
 jumbo frames, 17
 length/type, 17
 MAC addresses, 17, 18–20
 NIC, 18
 pads, 17

preambles, 17

start frame delimiters, 17

Ethernet packet frames, 17

check sequences, 17

components of (overview), 17

data, 17

data structure of, 17

destination MAC addresses and sources, 17

length/type, 17

MAC addresses, 17, 20

defined, 18

ipconfig/all command, 18–19

length of, 18

Linux, 20

macOS, 20

obtaining, 19–20

OUI, 18

sampling of, 18

Windows 10, 20

NIC

MAC addresses, 18

NIC, 18

teaming, 18

pads, 17

preambles, 17

start frame delimiters, 17

E-Tree (Ethernet Treet) service, 275–276

EVC (Ethernet Virtual Connections), 274

events, troubleshooting fiber-optic cabling, 162

evil twin attacks, 598

EXEC (privileged EXEC) passwords, 627

exit routes

Design and Construction Requirements for Exit Routes
(29 CFR 1910.36), 709–710

Maintenance, Safeguards, and Operational Features for
Exit Routes (29 CFR 1910.37), 710

export controls, international, 720–722

extending wireless ranges, 214

F

factory passwords, changing, 33

factory resets, 662

Fast Ethernet, 76

interface configurations, routers, 376–377

ports, 250, 263

fast-forward mode, switches, 247

FC (Fibre Channel), 699

FC connectors, fiber-optic cabling, 145–146

FCoE (Fibre Channel over Ethernet), 699

FERPA (Family Educational Rights and Privacy Act), 719

FHRP (First Hop Redundancy Protocol), 730

FHSS (Frequency-Hopping Spread Spectrum), 180

fiber Bragg grating, 139

fiber couplers, 64

fiber cross-connects, 151

fiber transceivers, 154

fiber-optic cabling. *See also* physical layer cabling

absorption, 136

advantages of, 126–127

APC connectors, 146

attenuation (insertion loss), 127, 136–137

attenuators, 142

backbones, 155

bandwidth, 126

BD fiber, 151–154

branching devices, 142

building distributions, 151–154

campus networks, 154–157

chromatic dispersion, 137–138

cladding, 130

color-coding fiber, 156

components of, 126, 141–142

connectorization, 145–146

cores, 130

corrosion, 127

costs, 127

crosstalk, 127

CWDM, 142

detectors, 143–145

DFB lasers, 141

diplexers, 154

dispersion, 137–139

dispersion compensation, 139

dispersion shifted fibers, 138–139

DL, 141

DWDM, 130, 141

electrostatic interference, 126

Ethernet, 157

events, troubleshooting, 162

FC connectors, 145–146

fiber, defined, 142

- fiber Bragg grating, 139
- fiber cross-connects, 151
- fiber selection, 132–133
- fiber-to-the-home/business, 130
- FTTB, 149
- FTTC, 149
- FTTD, 149
- FTTH, 149
- fusion splicing, 144
- GBIC, 152–153
- glass, 142
- graded-index fiber, 132, 133–134
- IC fibers, 152
- IDC, 152–153
- index-matching gel, 144
- IR (Infrared) radiation, 126
- isolators, 142
- LC connectors, 145–146
- LED, 141
- light pipes, 142
- link budgets, 157–158
- logical fiber maps, 154, 155
- mechanical splicing, 144–145
- microbending, 136–137
- mm fibers, 155
- modal dispersion, 137–138
- mode field diameters, 134–135
- MT-RJ connectors, 145–146
- multimode fiber, 130, 132
- numerical apertures, 131
- optical connectors, 126
- optical Ethernet, 149–150
- optical networking, defined, 148–151
- optical spectrum, 130–131
- optical-line amplifiers, 143
- OTDR, 162–163
- photosensitive detectors, 126
- physical fiber maps, 154, 156
- polarization mode dispersion, 137, 139
- pulse dispersions, 132–133
- refraction of light, 129
- refractive indexes, 129
- RSL, 142
- safety, 127, 160–161
- SC connectors, 145–146
- scattering, 136
- security, 127

- SFP, 152–153
- SFP+153–154
- “shooting the fiber”, 162
- single-mode fibers, 130, 134–135
- sm fibers, 155
- splitters, 142
- ST connectors, 145–146
- step-index fiber, 133
- strands, 131–132
- transceivers, 154
- transmission strands, 126
- troubleshooting, 162–163
- tunable lasers, 141–142
- “two-deep” rule, 152–153
- unconnected fibers, 146
- UPC connectors, 146
- VCSEL, 141
- VFL, 162
- WDM, 130, 143
- X2, 153–154
- XENPAK, 153–154
- XFP, 153–154
- XPAK, 153–154
- zero dispersion wavelengths, 138–139

fibers

- BD fiber, 151–154
- IC fibers, 152
- mm fibers, 155
- “shooting the fiber”, 162
- sm fibers, 155
- unconnected fibers, 146

fiber-to-the-home/business, 130

Fibre Channel (FC), 699

Fibre Channel over Ethernet (FCoE), 699

filtering

- BPDU Filter, 636
- content filters, 620
- MAC addresses, 33
- packets, 618
- traffic, 268
- web filters, 620

Fire Detection Systems (29 CFR 1910.164), 714–715

Fire Prevention Plans (29 CFR 1910.39), 711–712

firewalls, 34

- ACL, 617–618
- configuring, 611–617
- deploying, 619

- DMZ, 618
- NGFW, 620
- packet filtering, 618
- personal firewalls, 610
- proxy servers, 618
- screened subnets, 618
- SPI, 34
- stateful firewalls, 618
- FISMA (Federal Information Security Management Act), 719**
- Fixed Extinguishing Systems (29 CFR 1910.160), 713–714**
- flapping, route, 478**
- flash memory, 368**
- flat networks, 359**
- flooding, switches, 246**
- FLP (Fast Link Pulses), 383**
- forensics, computer, 621**
- forward DNS lookups, 539**
- forwarding, port, 35**
- forwarding state, STP, 423**
- FPP (Fire Prevention Plans), 711–712**
- fragment collisions, 247**
- fragment-free mode, switches, 247**
- frames, 17**
 - check sequences, 17
 - components of (overview), 17
 - data, 17
 - data structure of, 17
 - destination MAC addresses and sources, 17
 - jumbo frames, 17
 - length/type, 17
 - MAC addresses, 17, 20
 - defined, 18*
 - ipconfig/all command, 18–19*
 - length of, 18*
 - Linux, 20*
 - macOS, 20*
 - obtaining, 19–20*
 - OUI, 18*
 - sampling of, 18*
 - Windows 10, 20*
- NIC, 18
 - MAC addresses, 18*
 - teaming, 18*
- pads, 17
- preambles, 17
- start frame delimiters, 17

- frequencies, interference, troubleshooting, 214
- frequency bands, RFID tags, 203
- frequency channels, WLAN, 179
- FTP data packets, 566–567**
- FTTB (Fiber-To-The-Business), 149**
- FTTC (Fiber-To-The-Curb), 149**
- FTTD (Fiber-To-The-Desktop), 149**
- FTTH (Fiber-To-The-Home), 149**
- full backups, 730**
- full channels, 92**
- full-duplex cabling, 76**
- full-duplex mode, interfaces, 384–386**
- full-duplex transmissions, 100**
- fusion splicing, 144**
- F/UTP (Foil over Twisted-Pair Cabling), 99**

G

- gateways**
 - addresses, 265, 326–327, 359–361
 - default gateways, static routing, 448
 - FHRP, 730
 - of last resort, 454
 - voice gateways, 251
- gateways/broadband modems, 28**
- GBIC (Gigabit Interface Converters), 152–153**
- GDPR (General Data Protection Regulation), 719**
- geofencing, 204**
- giants, 433**
- Gigabit Ethernet, 76**
- glass, fiber-optic cabling, 142**
- GLBA (Gramm-Leach-Bliley Act), 719–720**
- graded-index fiber, 132, 133–134**
- GRE (Generic Routing Encapsulation), 648–649**
- gTLD, 528**
- guest machines, virtualization, 680**

H

- HA (Hardware Addresses), 302**
- HA (High Availability), 730–731**
- half-duplex mode, interfaces, 384–386**
- hand-offs, 178**
- handshakes, TCP, 298, 299**
- hardware addresses. *See* MAC addresses**
- hardware keys, 682**

hashing algorithms

MD5, 649, 650

SHA, 649, 650

Hazard Communication (29 CFR 1910.1200), 716

HC (Horizontal Cross-Connects), 68, 69

HDLC (High-Level Data Link Control), 272, 273

headends, VPN, 647

headers

IP headers, 301

TCP, 296–297

UDP headers, 300–301

hello packets, 477

help (?) command, 367

hexadecimal numbers, 309–311

HF (High Frequency) RFID tags, 203

hierarchy data rates, SONET/SDH, 149

hijacking sessions, 599

HIPAA (Health Insurance Portability and Accountability Act), 720

home access, home networks, 31

home networks, 24

appearance, 31

captive portals, 32

connecting, 32

cost, 30

data speeds, 30

ease of implementation, 31

encryption, 33

home access, 31

hotspots, 32

public access, 31

range extenders, 32

security, 33–34

troubleshooting, 31–32

wired networks

access points (AP), 28

advantages/disadvantages of, 24

broadband modems/gateways, 28

cable modems, 28, 29

components of, 25–30

defined, 24

DSL modems, 29–30

example of, 25

hubs, 25

network adapters, 26

routers, 26–27

switches, 26

wireless routers, 28

wireless networks (Wi-Fi), 24

access points (AP), 28

advantages/disadvantages of, 24

broadband modems/gateways, 28

cable modems, 28, 29

components of, 25–30

defined, 24

DSL modems, 29–30

example of, 25

hubs, 25

IEEE wireless standards, 24–25

network adapters, 26

routers, 26–27

switches, 26

Wi-Fi Alliance, 24–25

wireless routers, 25, 28

hop count metrics, 461, 463–464

hopping sequences, 180

hopping, VLAN, 599

horizontal cabling, 67, 69–73, 83–87

host (interface) identifiers, 335

host IP addresses, 315

host machines, virtualization, 680

host numbers, IP addressing, 21

hostname command, 374–375, 411–412

hostnames, 366

hot sites, disaster recovery, 731

“hot/cold” aisles, 73

hotspots, 32, 641

HSPA+ (Evolved High-Speed Packet Access), 204

HSSI (High-Speed Serial Interfaces), 270

hub-and-spoke topologies. *See* star topologies

hubs

broadcasts, 9

defined, 9

home networks, 25

link light indicators, 42

switches and, 10, 239–242

Token Ring hubs, 7

wireless routers, home networks, 28

HVAC systems, 717

hybrid clouds, 696

hybrid echo cancellation circuits, 100

Hyper-V, 682–690

hypervisors, 680

I

- IaaS (Infrastructure as a Service), 694**
- IANA (Internet Assigned Numbers Authority), 20, 528**
- IB (InfiniBand), 699**
- IC (Interconnect) fibers, 152**
- IC (Intermediate Cross-Connects), 68, 69**
- ICANN (Internet Corporation for Assigned Names and Numbers), 295, 529**
- ICMP (Internet Control Message Protocol), 46, 302–303**
- IDC (Intermediate Distribution Closets), 152–153**
- IDS (Intrusion Detection Systems), 619**
- IEEE (Institute of Electrical and Electronics Engineers), 7**
 - 802.1x (dot1x) wireless standard, 633
 - 802.11 wireless standard, 175–176
 - ad hoc networks, 176, 177*
 - AP, 177–178*
 - BSS, 176, 177, 178*
 - channel bonding, 179*
 - CSMA/CD, 178*
 - DSSS, 179*
 - ESS, 178*
 - FHSS, 180*
 - frequency channels, 179*
 - hand-offs, 178*
 - hopping sequences, 180*
 - ISM band, 179*
 - MAC layer, 176*
 - OFDM, 180*
 - Open Authentication, 638*
 - PHY layer, 176*
 - pseudorandom numbering sequences, 180*
 - roaming, 178*
 - shared-key authentication, 638*
 - transceivers, 177*
 - transmit power, 180*
 - WMN, 176*
 - 802.11a (Wi-Fi 2) wireless standard, 24, 180–181, 183
 - 802.11ac (Wi-Fi 5) wireless standard, 24, 182, 183
 - 802.11ax (Wi-Fi 6) wireless standard, 25, 182, 183
 - 802.11b (Wi-Fi 1) wireless standard, 24, 181, 183
 - 802.11g (Wi-Fi 3) wireless standard, 24, 181, 182, 183
 - 802.11i wireless standard, 183
 - 802.11n (Wi-Fi 4) wireless standard, 24, 181, 182, 183
 - 802.11r wireless standard, 183
 - 802.16a (WiMAX) wireless standard, 200
 - 802.3an-2006, 98
 - Wi-Fi Alliance, 24–25
 - wireless standards, 24–25
- IETF (Internet Engineering Task Force), 477**
- IGMP (Internet Group Management Protocol), 303–304**
- IKE (Internet Key Exchange), 651**
- implementing, home networks, 31**
- in-addr.arpa, 528**
- incident response policies, 725**
- incremental backups, 730**
- index-matching gel, 144**
- industry regulatory compliance, 718**
 - FERPA, 718
 - FISMA, 719
 - GDPR, 719
 - GLBA, 719–720
 - HIPAA, 720
 - international export controls, 720–722
 - PCI DSS, 720
- InfiniBand (IB), 699**
- infrastructure management**
 - DHCP deployments, 535–537
 - DNS, 539
 - dig command, 541*
 - forward DNS lookups, 539*
 - nslookup command, 541*
 - reverse DNS lookups, 539*
 - root DNS servers, 539–540*
 - RR, 541–546*
 - tree hierarchies, 539–540*
 - domain names, 528
 - FTP data packets, 566–567
 - IP address assignments, 529–530
 - IP addresses
 - assigning, 529–530*
 - managing with DHCP, 531–537*
 - IP networks, troubleshooting, 568–573
 - network management protocols, 546–551
 - network traffic analysis, 552–565
 - number resources, 529
 - protocol assignments, 529
 - scaling networks, 537–538
 - SFTP, 566
 - SNMP, 546–547
 - configuring, 547–551*
 - MIB, 547*

- SNMPv2, 550
- SNMPv3, 550
- Wireshark, 560–565
- inlays, RFID, 202**
- input errors, 432**
- input ports, 41**
- inquiry procedures, Bluetooth devices, 197**
- insertion loss (attenuation), 92, 93–94**
 - ACR, 93, 95
 - fiber-optic cabling, 127, 136–137, 142
 - PSAACRF, 98, 99
- PSACR, 93, 95, 96**
- .int, 528**
- interconnecting LAN**
 - access/edge layer, 269
 - bridges
 - advantages/disadvantages of, 236*
 - ARP caches, 233–235*
 - associations, 233*
 - broadcasts, 233*
 - defined, 232*
 - MAC addresses, 232–234*
 - multiport bridges. See layer 2 switches*
 - ports, 232–233*
 - translation bridges, 235*
 - transparent bridges, 235*
 - wireless bridges, 236*
 - Carrier Ethernet, 273–274
 - CSU/DSU, 272
 - data center architectures, 269
 - data channels, 270–271
 - distribution/aggregation layer, 269
 - E-LAN service, 275
 - E-Line, 274, 275
 - Ethernet service attributes, 276–277
 - Ethernet Service Definition, 274
 - E-Tree service, 275–276
 - EVC, 274
 - HDLC, 272, 273
 - lines of demarcation, 271
 - MEF, 274
 - MOE, 273–274
 - POP, 271
 - PPP, 272–273
 - routers, 262–266
 - auxiliary input, 250*
 - console input/cabling, 250*
 - console ports, 254–261*
 - FastEthernet ports, 250, 263*
 - gateway addresses, 265*
 - higher-end routers, VoIP, 252–253*
 - interfaces, 250–251*
 - logical addresses, 249*
 - MPLS, 252*
 - network addresses, 249*
 - packet shapers, 253*
 - ports, 249–250*
 - QoS, 251–253*
 - routing tables, 265*
 - segments, 265–266*
 - serial interfaces, 251*
 - serial ports, 264*
 - USB interfaces, 250*
 - VIC-4FXS/DID, 251*
 - voice interface cards, 251*
 - VoIP, 251*
 - WIC2AM, 251*
 - switches, 237–238, 239
 - adaptive cut-through mode, 247*
 - aging time, 244*
 - benefits of, 246*
 - broadcast domains, 246*
 - CNA, 242–243*
 - cut-through mode, 247*
 - dynamic assignments, 243*
 - error thresholds, 247*
 - fast-forward mode, 247*
 - flooding, 246*
 - fragment-free mode, 247*
 - hubs and, 239–242*
 - IP addressing, 245*
 - isolating collision domains, 246*
 - latency, 246*
 - layer 2 switches, 238*
 - managed switches, 242–247*
 - MLS, 247*
 - multicast messages, 239*
 - ports, 243*
 - secure addresses, 243*
 - stacked switches, 243–244*
 - static assignments, 243*
 - store-and-forward mode, 246*
 - wire speed routing, 247*
- traffic flows, 269

- UNI, 274
- WAN, 267–277
- interfaces**
 - auto-negotiation, 383–386
 - host interfaces, identifiers, 335
 - routers, 250–251
 - administratively down*, 390
 - full-duplex mode*, 384–386
 - half-duplex mode*, 384–386
 - troubleshooting*, 387–392
 - subinterfaces, VLAN, 418–419
 - UNI, 274
 - USB interfaces, 250
- interference**
 - fiber-optic cabling, 126
 - WLAN, troubleshooting*, 214
- international export controls, 720–722**
- Internet layer, TCP/IP, 294, 301**
 - ARP, 301–303
 - ICMP, 302–303
 - IGMP, 303–304
 - IP, 301
- intranets, 21, 316**
- intrusion attacks, 594–595**
 - brute-force attacks, 596
 - dictionary attacks, 596
 - packet sniffing attacks, 597–599
 - password cracking attacks, 596–597
 - social engineering attacks, 595–596
- inventory/asset management, 728**
- IoT (Internet of Things), 568, 662–663**
- IP (Internet Protocol)**
 - addressing. *See* separate entry
 - ip helper command, 533
 - IP internetworks, 21–22
 - ip route command, 451
 - security cameras, 662
 - telephony, 251
 - troubleshooting, 568–573
 - tunnels, 648
- IP (Internet Protocol), addressing**
 - APIPA, 532, 533
 - assigning, 529–530
 - gateway addresses, 326–327
 - headers, 301
 - IANA, 20
 - IPAM, 546
 - IPSec, 598, 651
 - IPv4, 312–313
 - 6to4 prefix*, 335
 - ARIN*, 315
 - assigning*, 315
 - A.B.C.D. values*, 20–21
 - class network addresses*, 467
 - classes*, 313
 - classful addresses*, 317
 - decimal/binary octets*, 314
 - default gateway addresses*, 359–361
 - dual stacks*, 336
 - host IP addresses*, 315
 - host numbers*, 21
 - network numbers*, 21
 - network/host bits*, 314–315
 - next hop addresses*, 362
 - non-Internet-routable IP addresses*, 316
 - private IP addresses*, 21–22, 316
 - public IP addresses*, 22
 - RIR*, 315
 - structure of*, 313
 - transitioning to IPv6*, 335–337
 - IPv6, 333–335, 337
 - 6to4 prefix*, 335
 - anycast addresses*, 335
 - CIDR*, 337–338
 - defined*, 333
 - dual stacks*, 336
 - interface (host) identifiers*, 335
 - IPng*, 333
 - link-local addresses*, 335, 336–337
 - multicast addresses*, 335
 - routing*, 499
 - routing, BGP*, 501–502
 - routing, EIGRP*, 501
 - routing, OSPF*, 500–501
 - routing, RIP*, 499–500
 - routing, static*, 499
 - SLAAC*, 336–337
 - transitioning to*, 335–337
 - unicast addresses*, 335
 - lease time, 532
 - managing with DHCP, 531–537
 - network numbers, 482
 - Office LAN, 40

overloading, 35
private IP addresses
 APIPA, 532, 533
 NAT, 34–35
public IP addresses, NAT, 35
switches, configuring, 245
TCP/IP, 21–22
troubleshooting, 570
VM, 682
wildcard bits, 482–483

IPAM (IP Address Management), 546

ipconfig command, LAN testing/troubleshooting, 47–48

ipconfig /release command, 532

ipconfig /renew command, 532

ipconfig/all command, 18–19, 39

IPng (IP Next Generation), 333

IPS (Intrusion Prevention Systems), 619

IPSec, 598, 651

IR (Infrared) radiation, 126, 130

ISAKMP (Internet Security Association and Key Management Protocol), 651

iSCSI (Internet Small Computer Systems Interface), 699

IS-IS (Intermediate System-to-Intermediate System), 478–479

ISM (Industrial, Scientific, Medical) band, 179

isolating

 collision domains, 246

network problems, 14

isolators, fiber-optic cabling, 142

ISP (Internet Service Providers), defined, 21

IT audits, 728

J

jamming wireless networks, 638

jitter, 252

jumbo frames, 17

K

keepalive packets, 388

Kerberos authentication, 623

key exchanges

 Diffie-Hellman key exchange, 651

 IKE, 651

 ISAKMP, 651

keys, hardware, 682

L

L2F (Layer 2 Forwarding) protocol, 650

L2TP (Layer 2 Tunneling Protocol), 650, 651

labeling, 71–72

 port labeling, 72

 system labeling, 72

LACP (Link Aggregation Control Protocol), 424

LAN (Local Area Networks), 5, 6. *See also* VLAN; WLAN

 access/edge layer, 269

 bridges

advantages/disadvantages of, 236

ARP caches, 233–235

associations, 233

broadcasts, 233

defined, 232

MAC addresses, 232–234

*multiport bridges. *See* layer 2 switches*

ports, 232–233

translation bridges, 235

transparent bridges, 235

wireless bridges, 236

 Carrier Ethernet, 273–274

 core layer, 268

 CSU/DSU, 272

 data center architectures, 269

 data channels, 270–271

 default gateway addresses, 359–361

 distribution/aggregation layer, 269

 E-LAN service, 275

 E-Line, 274, 275

 Ethernet LAN, 16

cabling, numerics, 41

CSMA/CD, 16

frames, 17

 Ethernet service attributes, 276–277

 Ethernet Service Definition, 274

 E-Tree service, 275–276

 EVC, 274

 flat networks, 359

 HDLC, 272, 273

 interconnecting WAN, 267–277

 layer 3 networks, 359–364

 lines of demarcation, 271

 MEF, 274

 MOE, 273–274

- Office LAN, assembling, 38–39
 - cabling*, 40–43
 - client/server networks*, 42–45
 - configuring computers for LAN operation*, 44
 - diagramming networks*, 39–40
 - IP addressing*, 40
 - MAC addresses*, 40
 - network device connections*, 40–43
 - peer-to-peer networks*, 42, 43
- POP, 271
- PPP, 272–273
- routers
 - auxiliary input*, 250
 - console input/cabling*, 250
 - console ports*, 254–261
 - FastEthernet ports*, 250, 263
 - gateway addresses*, 265
 - higher-end routers, VoIP*, 252–253
 - interconnecting LAN*, 262–266
 - interfaces*, 250–251
 - logical addresses*, 249
 - MPLS*, 252
 - network addresses*, 249
 - packet shapers*, 253
 - ports*, 249–250
 - QoS*, 251–253
 - routing tables*, 265
 - segments*, 265–266
 - serial interfaces*, 251
 - serial ports*, 264
 - USB interfaces*, 250
 - VIC-4FXS/DID*, 251
 - voice interface cards*, 251
 - VoIP*, 251
 - WIC2AM*, 251
- switches, 237–238, 239
 - adaptive cut-through mode*, 247
 - aging time*, 244
 - benefits of*, 246
 - broadcast domains*, 246
 - CNA*, 242–243
 - cut-through mode*, 247
 - dynamic assignments*, 243
 - error thresholds*, 247
 - fast-forward mode*, 247
 - flooding*, 246
 - fragment-free mode*, 247
 - hubs and*, 239–242
 - IP addressing*, 245
 - isolating collision domains*, 246
 - latency*, 246
 - layer 2 switches*, 238
 - managed switches*, 242–247
 - MLS*, 247
 - multicast messages*, 239
 - ports*, 243
 - secure addresses*, 243
 - stacked switches*, 243–244
 - static assignments*, 243
 - store-and-forward mode*, 246
 - wire speed routing*, 247
- testing, 45–48
- traffic flows, 269
- troubleshooting, 45–48
- UNI, 274
- language table registries, 528**
- last resort, gateways of, 454**
- last-mile connections, 200**
- latency**
 - metrics, 461
 - network latency, 252
 - switches, 246
- layer 2 switches, 238**
- layer 3 networks, 359–364**
- LC connectors, fiber-optic cabling, 145–146**
- LCL (Longitudinal Conversion Loss), 99**
- LEAP (Lightweight Extensible Authentication Protocol), 640**
- learning state, STP, 423**
- lease time, 532**
- LED (Light-Emitting Diodes), 141**
- length/type, frames, 17**
- LF (Low Frequency) RFID tags, 203**
- licenses, MLA, 724**
- light**
 - electromagnetic wavelength spectrum, 131
 - IR (Infrared) radiation, 126, 130
 - optical spectrum, 130–131
 - refraction of, 129
 - refractive indexes, 129
 - light detectors, fiber-optic cabling, 143–145
 - light pipes, defined, 142

- line console passwords, 375–376, 412–414
- line passwords, 626–627
- lines of demarcation, 271
- link budgets, 157–158
- link integrity tests, 42
- link light indicators, 42
- link-local addresses, 335, 336–337
- link (port) aggregation, 424
- link pulses, 42
- link state protocols, 476–477
 - EIGRP, 487–494, 501
 - IS-IS, 478–479
 - LSA, 477
 - NET addresses, 479
 - OSPF, 477, 483–486
 - advantages/disadvantages of, 478
 - Area 0, 482
 - areas, 477
 - configuring, 481–485
 - hello packets, 477
 - IPv6, 500–501
 - router ospf [process id] command, 481
 - VLSM, 478
 - RIP and, 477
 - route flapping, 478
- links, cabling, 92
- Linux
 - firewalls, 616–617
 - MAC addresses, obtaining, 20
- listening state, STP, 423
- Live Migration, 681
- load balancing, dynamic routing protocols, 460
- load issues (WLAN), troubleshooting, 215
- load metrics, 461
- lockers, smart, 663
- locking cabinets, 661
- locking racks, 661
- locks, racks, 73
- logging, routers, 630–631
- logic bombs, 604
- logical addresses, 249
- logical fiber maps, 154, 155
- long hauls, data transmissions, 134
- lookups, DNS, 539
- loopbacks, 448–449
- loops, routing, 465

- loss of association, WLAN, 193
- LSA (Link State Advertisements), 477
- LTE/4G, 204

M

- MAC (Media Access Control) layer, 802.11 wireless standard, 176

- MAC addresses, 20

- aging time, 244
- bridges, 232–234
- CAM, 246
- defined, 17, 18
- destination MAC addresses and sources, 17
- dynamic assignments, 243
- filtering, 33
- ipconfig/all command, 18–19
- length of, 18
- Linux, 20
- macOS, 20
- NIC, 18
- obtaining, 19–20
- Office LAN, 40
- OUI, 18
- sampling of, 18
- spoofing attacks, 635
- static assignments, 243
- sticky command option, 634
- Windows 10, 20

- macOS

- firewalls, 615–616
- home networks, connecting, 32
- MAC addresses, obtaining, 20
- remote client VPN configurations, 652–653
- ZTerm serial communications software, 259–261

- magic numbers, subnetting, 323

- Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37), 710

- malware

- antivirus/anti-malware software, 610–611
- logic bombs, 604
- ransomware attacks, 604
- viruses, 602–603
- worms, 603
- zero-day attacks, 604

- MAN (Metropolitan Area Networks), 5

managed switches, 242–247

managing

- asset/inventory management, 728
- cabling, 67
- change management policies, 624
- domain names, 528
- inventory/asset management, 728
- IP addressing, IPAM, 546
- network access, 623–624
- network infrastructures
 - DHCP deployments, 535–537*
 - DNS, 539–546*
 - domain names, 528*
 - FTP data packets, 566–567*
 - IP address assignments, 529–530*
 - IP address management with DHCP, 531–537*
 - network management protocols, 546–551*
 - number resources, 529*
 - protocol assignments, 529*
 - scaling networks, 537–538*
 - SFTP, 566*
 - SNMP, 546–551*
 - traffic analysis, 552–565*
 - troubleshooting IP networks, 568–573*
 - Wireshark, 560–565*
- number resources, 529

man-in-the-middle attacks (on-path attacks), 598

mantraps (access control vestibules), 661

manufacturer’s specifications, cabling, 102–104

mapping, ports, 35

maps

- color maps, T568A/T568B wiring standards, 78–80
- logical fiber maps, 154, 155
- physical fiber maps, 154, 156
- wiremaps, 82

MC (Main Cross-Connects), 68, 69

MD5 (Message Digest 5) hashing algorithm, 649, 650

mechanical splicing, 144–145

media converters, 262–263

MEF (Metro Ethernet Forum), 274

memory

- CAM, 246
- flash memory, 368

mesh topologies, 10–11

metrics, dynamic routing protocols, 460, 461

mGRE (Multipoint GRE), 649

MIB (Management Information Bases), 547

microbending, fiber-optic cabling, 136–137

MIMO (Multiple-Input Multiple-Output), 182

MLA (Master License Agreements), 724

MLS (Multilayer Switches), 247

mm (multimode) fibers, 155

mobile (cellular) communications, 204

- 3G wireless standard, 204
- 4G wireless standard, 204
- 5G wireless standard, 204
- CDMA, 204
- EDGE, 204
- geofencing, 204
- HSPA+204
- LTE/4G, 204
- NFC, 204

modal dispersion, 137–138

mode field diameters, 134–135

modems

- ADSL modems, 645–646
- analog modems
 - asymmetric operations, 643*
 - security, 643–644*
 - V.44/V.34 modem standard, 643*
 - V.92/V.90 modem standard, 643*
- broadband modems/gateways, 28
- cable modems
 - DSL modems, 29–30*
 - home networks, 28, 29*
 - security, 644*
- dialup modems, 644
- xDSL modems, security, 644–646

MOE (Metro Optical Ethernet), 273–274

motion detection, 662

MOU (Memorandums of Understanding), 723–724

Mpbs (Megabits per second), 40

MPLS (Multiprotocol Label Switching), 252

MSA (Master Service Agreements), 724

MSDS (Material Safety Data Sheets), 716

MSTI (Multiple Spanning Tree Instances), 423–424

MSTP (Multiple Spanning Tree Protocol), 423–424

MT ACK, 534

MT Discover, 534

MT Offer, 534

MT Request, 534

MTBF (Mean Time Between Failures), 729
MT-RJ connectors, fiber-optic cabling, 145–146
MTTF (Mean Time To Failure), 729
MTTR (Mean Time To Recover/Repair), 729
multicast addresses, 335
multicast messages, 239
multicasting, 303
multilevel encoding, 100
multimeters, 110
multimode fiber, 130, 132
multiplexing, 271
 CWDM, 142
 DWDM, 130, 141
 OFDM, 180, 200
 WDM, 130
multipoint antenna distributions, 209–211
multiport bridges. *See* layer 2 switches
multiport repeaters. *See* hubs
multitenancy, cloud computing, 695, 696
MU-MIMO (Multiuser-MIMO), 182
MX records (Mail Exchange records), 543–544, 693

N

NAC (Network Access Control), 624
name resolution, troubleshooting, 571
NAS (Network Attached Storage), 700
NAT (Network Address Translation), 34
 defined, 34
 private IP addresses, 34–35
 public IP addresses, 35
 scaling networks, 537–538
NCP (Network Control Protocol), 292
NDA (Non-Disclosure Agreements), 725
near-end testing, 94
NET (Network Entity Title) addresses, 479
NET, subnet, 363
netstat -a command, 600
netstat -b command, 601
netstat -r command, 448
network adapters, home networks, 26
network addresses, 249, 322
network bridges. *See* bridges
Network interface layer, TCP/IP, 294, 304
Network layer, OSI model, 13
network numbers, IP addressing, 21, 482

network switches. *See* switches
network/host bits, IPv4 addressing, 314–315
networks
 access management, 623–624
 ad hoc networks, 176, 177
 campus network hierarchical topologies, 69
 campus networks
 backbones, 477
 defined, 230
 optical networking, 154–157
 CAN, 5
 client/server networks, 42–45
 congestion (bottlenecking), 76, 252
 connections, verifying with ping command, 240–241
 contiguous networks, 467
 deterministic networks, 7
 diagramming, 39–40
 enterprise networks, 5, 262
 flat networks, 359
 home networks, 24
 appearance, 31
 captive portals, 32
 connecting, 32
 cost, 30
 data speeds, 30
 ease of implementation, 31
 encryption, 33
 home access, 31
 hotspots, 32
 NAT, 34–36
 public access, 31
 range extenders, 32
 security, 33–34
 troubleshooting, 31–32
 infrastructure management
 DHCP deployments, 535–537
 DNS, 539–546
 domain names, 528
 FTP data packets, 566–567
 IP address assignments, 529–530
 IP address management with DHCP, 531–537
 network management protocols, 546–551
 number resources, 529
 protocol assignments, 529
 scaling networks, 537–538
 SFTP, 566

- traffic analysis*, 552–565
- troubleshooting IP networks*, 568–573
- Wireshark*, 560–565
- interfaces, auto-negotiation, 383–386
- intranet, 21
- IP internetworks, 21–22
- IP networks, troubleshooting, 568–573
- isolating problems, 14
- LAN, 5, 6
 - assembling*, 38–43
 - bridges*, 232–236
 - configuring computers for LAN operation*, 44
 - console port connections*, 254–261
 - default gateway addresses*, 359–361
 - Ethernet LAN*, 16–23
 - flat networks*, 359
 - routers*, 249–253, 262–266
 - switches*, 237–238
 - testing*, 45–48
 - troubleshooting*, 45–48
 - WAN interconnections*, 267–277
- latency, 252
- layer 3 networks, 359–364
- MAN, 5
- management protocols, 546–551
- NAS, 700
- optical networking, 147–148
 - backbones*, 155
 - BD fiber*, 151–154
 - building distributions*, 151–154
 - campus networks*, 154–157
 - color-coding fiber*, 156
 - defined*, 148–151
 - diplexers*, 154
 - Ethernet*, 157
 - fiber cross-connects*, 151
 - FTTB*, 149
 - FTTC*, 149
 - FTTD*, 149
 - FTTH*, 149
 - GBIC*, 152–153
 - IC fibers*, 152
 - IDC*, 152–153
 - link budgets*, 157–158
 - logical fiber maps*, 154, 155
 - mm fibers*, 155
 - optical Ethernet*, 149–150
 - physical fiber maps*, 154, 156
 - SFP*, 152–153
 - SFP+*, 153–154
 - sm fibers*, 155
 - SONET/SDH*, 148–149
 - transceivers*, 154
 - “two-deep” rule*, 152–153
 - X2*, 153–154
 - XENPAK*, 153–154
 - XFP*, 153–154
 - XPAK*, 153–154
- OSI model, 12
 - Application layer*, 13, 14
 - Data link layer*, 13
 - layer numbers*, 13
 - layers, summary of*, 12–13
 - Network layer*, 13
 - Physical layer*, 13
 - Presentation layer*, 13–14
 - Session layer*, 13
 - Transport layer*, 13
- PAN, 4
- peer-to-peer networks, 42, 43
- PSTN, 251
- SAN, 698–699
- scaling, 537–538
- SDN, 696–697
- SD-WAN, 697
- security
 - ARP cache poisoning*, 598
 - brute-force attacks*, 596
 - buffer overflow attacks*, 599–600
 - dictionary attacks*, 596
 - DoS attacks*, 606–609
 - DTLS protocol*, 598
 - evil twin attacks*, 598
 - intrusion attacks*, 594–604
 - IPSec*, 598
 - malware*, 602–604
 - on-path attacks (man-in-the-middle attacks)*, 598
 - packet sniffing attacks*, 597–599
 - password cracking attacks*, 596–597
 - session hijacking*, 599
 - social engineering attacks*, 595–596
 - software vulnerabilities*, 599–604
 - SSL protocol*, 597–598
 - TLS protocol*, 598

- TTLS protocol*, 598
 - VLAN hopping*, 599
- segments, 265–266
 - defined*, 246
 - subnet, NET*, 363
- slowdowns, 233
- topologies, 7
 - bus topologies*, 8–9
 - defined*, 6
 - hub-and-spoke topologies*. See *star topologies*
 - mesh topologies*, 10–11
 - point-to-point topologies*, 6
 - star topologies*, 9, 10, 39
 - Token Ring topologies*, 6, 7–8
- traffic analysis, 552–565
- troubleshooting
 - bottom-to-top (bottom-up) approach*, 569
 - divide-and-conquer approach*, 569
 - isolating problems*, 14
 - spot-the-difference approach*, 569
 - top-to-bottom (top-down) approach*, 569
- verifying settings, 570
- VPN, 34
 - CHAP*, 649, 650
 - client-to-site VPN*, 648
 - EAP*, 650
 - GRE*, 648–649
 - headends*, 647
 - IP tunnels*, 648
 - IPSec*, 651
 - L2F*, 650
 - L2TP*, 650
 - MD5 hashing algorithm*, 649, 650
 - mGRE*, 649
 - PAP*, 649–650
 - PPP*, 649
 - PPTP*, 650
 - remote access VPN*, 648
 - remote client configurations*, 652–657
 - SHA*, 649, 650
 - site-to-site VPN*, 648
 - tunneling protocols*, 648–651
- WAN, 5
 - defined*, 526
 - example of*, 526
 - HSSI*, 270

- interconnecting LAN*, 267–277
 - LAN interactions*, 267–277
 - OC*, 270
 - SD-WAN*, 697
- wired networks
 - access points (AP)*, 28
 - advantages/disadvantages of*, 24
 - appearance*, 31
 - broadband modems/gateways*, 28
 - cable modems*, 28, 29
 - components of*, 25–30
 - cost*, 30
 - data speeds*, 30
 - defined*, 24
 - DSL modems*, 29–30
 - ease of implementation*, 31
 - example of*, 25
 - home access*, 31
 - hubs*, 25
 - network adapters*, 26
 - public access*, 31
 - routers*, 26–27
 - switches*, 26
 - troubleshooting*, 31–32
 - wireless routers*, 28
- wireless networks (Wi-Fi), 24
 - access points (AP)*, 28
 - advantages/disadvantages of*, 24
 - appearance*, 31
 - broadband modems/gateways*, 28
 - cable modems*, 28, 29
 - captive portals*, 32
 - components of*, 25–30
 - connecting*, 32
 - cost*, 30
 - data speeds*, 30
 - defined*, 24
 - DSL modems*, 29–30
 - ease of implementation*, 31
 - encryption*, 33
 - example of*, 25
 - firewalls*, 34
 - home access*, 31
 - hotspots*, 32
 - hubs*, 25
 - IEEE wireless standards*, 24–25

IP addressing, 34–36

NAT, 34–36

network adapters, 26

public access, 31

range extenders, 32

routers, 26–27

security, 33–34

switches, 26

troubleshooting, 31–32

VPN, 34

Wi-Fi Alliance, 24–25

wireless routers, 25, 28

wireless standards, 32

WMN, 176

WSN, ANT+ wireless technology, 183

NEXT (Near-End Crosstalk), 92, 93, 94–95; 98, 99

next hop addresses, 362

NFC (Near Field Communication), 204

NFPA (National Fire Protection Association), 709

NGFW (Next-Generation Firewalls), 620

NIC (Network Interface Cards)

defined, 18

MAC addresses, 18

teaming, 18

NLOS (Non-Line-Of-Sight), 200

nmap command, 601–602

no shutdown (no shut) command, 377

non-Internet-routable IP addresses, 316

NS records (Name Server records), 543

nslookup command, 541

NTP (Network Time Protocol), 630

number conversions

binary-to-decimal conversions, 306–307

decimal-to-binary conversions, 307–309

hexadecimal numbers, 309–311

number resources, managing, 529

numerical apertures, 131

numerics, Ethernet LAN cabling, 41

O

OC (Optical Carriers), 270

OFDM (Orthogonal Frequency-Division Multiplexing), 180, 200

offboarding/onboarding policies, 727

Office LAN, assembling, 38–39

cabling, 40–43

client/server networks, 42–45

configuring computers for LAN operation, 44

diagramming networks, 39–40

IP addressing, 40

MAC addresses, 40

network device connections, 40–43

peer-to-peer networks, 42, 43

omnidirectional antennas, 209

onboarding/offboarding policies, 727

on-path attacks (man-in-the-middle attacks), 598

Open Authentication, 638

optical beam splitters. See WDM

optical communications, fiber-optic cabling

absorption, 136

advantages of, 126–127

APC connectors, 146

attenuation (insertion loss), 127, 136–137

attenuators, 142

backbones, 155

bandwidth, 126

BD fiber, 151–154

branching devices, 142

building distributions, 151–154

campus networks, 154–157

chromatic dispersion, 137–138

cladding, 130

color-coding fiber, 156

components of, 126, 141–142

connectorization, 145–146

cores, 130

corrosion, 127

costs, 127

crosstalk, 127

CWDM, 142

detectors, 143–145

DFB lasers, 141

diplexers, 154

dispersion, 137–139

dispersion compensation, 139

dispersion shifted fibers, 138–139

DL, 141

DWDM, 130, 141

electrostatic interference, 126

- Ethernet, 157
- events, troubleshooting, 162
- FC connectors, 145–146
- fiber, defined, 142
- fiber Bragg grating, 139
- fiber cross-connects, 151
- fiber selection, 132–133
- fiber-to-the-home/business, 130
- FTTB, 149
- FTTC, 149
- FTTD, 149
- FTTH, 149
- fusion splicing, 144
- GBIC, 152–153
- glass, 142
- graded-index fiber, 132, 133–134
- IC fibers, 152
- IDC, 152–153
- index-matching gel, 144
- IR (Infrared) radiation, 126
- isolators, 142
- LC connectors, 145–146
- LED, 141
- light pipes, 142
- link budgets, 157–158
- logical fiber maps, 154, 155
- mechanical splicing, 144–145
- microbending, 136–137
- mm fibers, 155
- modal dispersion, 137–138
- mode field diameters, 134–135
- MT-RJ connectors, 145–146
- multimode fiber, 130, 132
- numerical apertures, 131
- optical connectors, 126
- optical Ethernet, 149–150
- optical networking, defined, 148–151
- optical spectrum, 130–131
- optical-line amplifiers, 143
- OTDR, 162–163
- photosensitive detectors, 126
- physical fiber maps, 154, 156
- polarization mode dispersion, 137, 139
- pulse dispersions, 132–133
- refraction of light, 129
- refractive indexes, 129
- RSL, 142
- safety, 127, 160–161
- SC connectors, 145–146
- scattering, 136
- security, 127
- SFP, 152–153
- SFP+153–154
- “shooting the fiber”, 162
- single-mode fibers, 130, 134–135
- sm fibers, 155
- splitters, 142
- ST connectors, 145–146
- step-index fiber, 133
- strands, 131–132
- transceivers, 154
- transmission strands, 126
- troubleshooting, 162–163
- tunable lasers, 141–142
- “two-deep” rule, 152–153
- unconnected fibers, 146
- UPC connectors, 146
- VCSEL, 141
- VFL, 162
- WDM, 130, 143
- X2, 153–154
- XENPAK, 153–154
- XFP, 153–154
- XPAK, 153–154
- zero dispersion wavelengths, 138–139

optical connectors, 126

optical Ethernet, 149–150

optical link budgets, 157–158

optical networking, 147–148

- backbones, 155
- BD fiber, 151–154
- building distributions, 151–154
- campus networks, 154–157
- color-coding fiber, 156
- defined, 148–151
- diplexers, 154
- Ethernet, 157
- fiber cross-connects, 151
- FTTB, 149
- FTTC, 149
- FTTD, 149
- FTTH, 149

- GBIC, 152–153
- IC fibers, 152
- IDC, 152–153
- link budgets, 157–158
- logical fiber maps, 154, 155
- mm fibers, 155
- optical Ethernet, 149–150
- physical fiber maps, 154, 156
- SFP, 152–153
- SFP+ 153–154
- sm fibers, 155
- SONET/SDH, 148
 - hierarchy data rates, 149*
 - STS, 149*
- transceivers, 154
- “two-deep” rule, 152–153
- X2, 153–154
- XENPAK, 153–154
- XFP, 153–154
- XPAK, 153–154
- optical spectrum, light, 130–131**
- optical transceivers, 154**
- optical-line amplifiers, fiber-optic cabling, 143**
- OSH (Occupational Safety and Health) Act, 708–709**
- OSHA (Occupational Safety and Health Administration), 708–709**
- OSI (Open Systems Interconnection) model, 12**
 - Application layer, 13, 14
 - Data link layer, 13
 - layers
 - numbers, 13*
 - summary of, 12–13*
 - Network layer, 13
 - Physical layer, 13
 - Presentation layer, 13–14
 - Session layer, 13
 - Transport layer, 13
- OSPF (Open Shortest Path First), 477, 483–486**
 - advantages/disadvantages of, 478
 - Area 0, 482
 - areas, 477
 - configuring, 481–485
 - hello packets, 477
 - IPv6, 500–501
 - router ospf [process id] command, 481
 - VLSM, 478

- OTDR (Optical Time-Domain Reflectometers), 162–163**
- OUI (Organizationally Unique Identifiers), 18, 304**
- outsourcing, cloud computing, 692**
- overloading, 35**

P

- PA (Protocol Addresses), 301**

- PaaS (Platform as a Service), 695**

- packet frames, 17**

- check sequences, 17
- components of (overview), 17
- data, 17
- data structure of, 17
- destination MAC addresses and sources, 17
- jumbo frames, 17
- length/type, 17
- MAC addresses, 17, 20
 - defined, 18*
 - ipconfig/all command, 18–19*
 - length of, 18*
 - Linux, 20*
 - macOS, 20*
 - obtaining, 19–20*
 - OUI, 18*
 - sampling of, 18*
 - Windows 10, 20*

- NIC

- MAC addresses, 18*
- NIC, 18*
- teaming, 18*

- pads, 17

- preambles, 17
- start frame delimiters, 17

- packet shapers, 253, 620**

- packets**

- ACK packets, 297
- ARP packets, 302–303
- DHCP packets, 534
- error thresholds, 247
- filtering, 618
- FTP data packets, 566–567
- hello packets, 477
- ICMP source-quench packets, 302
- IGMP packets, 303–304
- keepalive packets, 388

- shaping, 620
- sniffing attacks, 597–599
- SYN ACK packets, 297
- SYN packets, 297
- TCP packets
 - terminating connections*, 299–300
 - transmitting*, 298
- UDP packet transfers, 300–301
- WEP, 638–639
- wire speed routing, 247
- pads, defined, 17**
- paging procedures, Bluetooth devices, 197**
- PAN (Personal Area Networks), 4**
- PAP (Password Authentication Protocol), 649–650**
- parabolic reflector (dish) antennas, 209**
- passing tokens, 7**
- passive RFID tags, 201–202**
- passwords**
 - brute-force attacks, 596
 - cracking attacks, 596–597
 - dictionary attacks, 596
 - EXEC (privileged EXEC) passwords, 627
 - factory passwords, changing, 33
 - line console passwords, 375–376, 412–414
 - line passwords, 626–627
 - packet sniffing attacks, 597–599
 - PAP, 649–650
 - policies, 726
- PAT (Port Address Translation), 35, 538**
- patch cabling, 71–72, 82, 87–90**
- path determination, dynamic routing protocols, 460**
- PBX (Private Branch Exchanges), 251**
- PCI DSS (Payment Card Industry Data Security Standard), 720**
- PD (Powered Devices), 426, 427**
- PDoS (Permanent DoS) attacks, 607**
- PDU (Protocol Data Units), 730–731**
- peer-to-peer networks, 42, 43**
- penetration testing, 602**
- performance**
 - 10GBASE-T cabling, 100–101
 - cabling, 110
 - slowdowns, network, 233
- personal firewalls, 610**

- photodetectors. See detectors**
- photosensitive detectors, fiber-optic cabling, 126**
- PHY (Physical) layer, 802.11 wireless standard, 176**
- physical addresses. See MAC addresses**
- physical fiber maps, 154, 156**
- physical layer cabling, 64. See also fiber-optic cabling; twisted-pair cabling**
 - APC connectors, 64
 - BNC connectors, 64
 - connectors, 64
 - fiber couplers, 64
 - structured cabling
 - backbone cabling*, 67
 - building entrances*, 66–67
 - ER*, 67
 - HC*, 68, 69
 - horizontal cabling*, 67, 69–73
 - IC*, 68, 69
 - MC*, 68, 69
 - TCO*, 67
 - telecommunications closets*, 67, 69–70
 - TIA/EIA 568-A cabling standard*, 66
 - TIA/EIA 568-B cabling standard*, 66
 - TIA/EIA 569B cabling standard*, 66–67
 - WO*, 68
 - work areas*, 67
 - UPC connectors, 64
 - UTP couplers, 64
- Physical layer, OSI model, 13**
- physical security, 659, 660**
 - access control, 659, 660–661
 - access control vestibules (mantraps)*, 661
 - badge readers*, 661
 - biometric scanners*, 661
 - locking cabinets*, 661
 - locking racks*, 661
 - asset disposal, 662
 - biometric scanners, 661, 717
 - control devices, 660
 - detection methods, 661–662
 - motion detection*, 662
 - surveillance cameras*, 662
 - door access, 717
 - surveillance, 659
 - testing, 659
- piconets, 197–198**

- ping command, 14, 45–47, 240–241, 302–303
- pinouts, T568A/T568B wiring standards, 79
- PoE (Power over Ethernet), 425–428
- PoE+427
- PoE++428
- point-to-point topologies, 6
- poisoning ARP caches, 598
- polarization mode dispersion, 137, 139
- POP (Points of Presence), 271
- port (link) aggregation, 424
- Portable Fire Extinguishers (29 CFR 1910.157), 712–713
- port-based VLAN, 407
- ports
 - bridges, 232–233
 - common applications and port numbers, 295–296
 - console ports, routers
 - console cabling, 255
 - DB-9 connectors, 254–255
 - DB-25 connectors, 254, 255
 - PuTTY software, 256–259
 - RJ-45 connectors, 255
 - rollover cabling, 255–256
 - RS-232 serial communications ports, 254, 255
 - serial interfaces, 256
 - ZTerm serial communications software, 259–261
 - defined, 9
 - FastEthernet ports, 250, 263
 - forwarding, 35
 - input ports, 41
 - labeling, 72
 - mapping, 35
 - PAT, 35
 - private (dynamic) ports, 295
 - registered ports, 295
 - routers, 249–250
 - RS-232 serial communications ports, 254, 255
 - serial ports, 264
 - straight-through ports, 42
 - switches, 243, 431–432, 633–635
 - TCP ports, 573
 - TCP/IP, 295
 - trunk ports, 408–409
 - UDP ports, 573
 - uplink ports, 42
 - VLAN port assignments, 431
 - well-known (reserved) ports, 295

- PPP (Point-to-Point Protocol), 272–273, 649
- PPTP (Point-to-Point Tunneling Protocol), 650
- preambles, defined, 17
- Presentation layer, OSI model, 13–14
- printers, wireless printers, troubleshooting, 216
- private clouds, 696
- private (dynamic) ports, 295
- private IP addresses, 21–22, 316
 - APIPA, 532, 533
 - NAT, 34–35
- Privileged EXEC mode (Router#), 373–381
- privileged mode
 - routers, 373
 - switches, 411, 412
- privileged user agreements, 726
- propagation delay, 93, 96
- protocol-based VLAN, 408
- protocols
 - assigning, 529
 - defined, 6
 - ICMP, 46
- proxy servers, 618
- PSAACRF (Power-Sum Alien ACRF), 98, 99
- PSACR (Power-Sum Attenuation to Crosstalk Ratios), 93, 95, 96
- PSANEXT (Power-Sum Alien NEXT), 98, 99
- PSE (Power Sourcing Equipment), 426–427
- PSELFEXT (Power-Sum ELFEXT), 93, 95, 96
- pseudorandom numbering sequences, 180
- PSNEXT (Power-Sum NEXT), 93, 94
- PSTN (Public-Switched Telephone Networks), 251
- PTR records (Pointer records), 542
- public access, home networks, 31
- public clouds, 696
- public IP addresses, 22, 35
- pulse dispersions, 132–133
- PuTTY software, configuring, 256–259
- PVST (Per-VLAN Spanning Tree), 423–424

Q - R

- QoS (Quality of Service), VoIP, 251–253
- queuing/buffering, 252
- racks
 - diagrams, 72
 - locks, 73, 661

- RADIUS (Remote Authentication Dial-In User Service), 624, 640**
- range command, 633**
- ranges (wireless), extending, 32, 195, 214**
- ranging, cable modems, 644**
- ransomware attacks, 604**
- RAS (Remote Access Servers), 647**
- RBAC (Role-Based Access Control), 623**
- readers, RFID, 201**
- recovery/continuity policies/procedures, 729**
 - MTBF, 729
 - MTTF, 729
 - MTTR, 729
- redundancy**
 - circuits, 730
 - FHRP, 730
- reflective/amplified DoS attacks, 608**
- refraction of light, 129**
- refractive indexes, 129**
- registered ports, 295**
- reliability metrics, 461**
- remote access security, 642**
 - analog modems, 643–644
 - cable modems, 644
 - RAS, 647
 - xDSL modems, 644–646
- remote access VPN, 648**
- remote antenna installations, 211**
- remote client VPN configurations, 652–657**
- remote desktops, 695**
- replies, ARP, 301–303**
- requests, ARP, 301–302**
- reserved (well-known) ports, 295**
- resets, factory, 662**
- return loss, testing, 93, 95–96**
- reverse DNS lookups, 539**
- RF signal strength, WLAN, 191–195, 209–211**
- RFID (Radio Frequency Identification), 200, 201**
 - backscatter, 200
 - block diagram, 200–201
 - inlays, 202
 - readers, 201
 - tags, 200
 - active tags, 202*
 - communications (air interface) portal, 203*
 - frequency bands, 203*
 - HF tags, 203*
 - LF tags, 203*
 - passive tags, 201–202*
 - semi-active tags, 202*
 - Slotted Aloha, 203*
 - UHF tags, 203*
- RIP (Routing Information Protocol), 465**
 - configuring, 466–468
 - IPv6, 499–500
 - link state protocols and, 477
 - [rip_tag] tags, 500
 - route configuration, 468–473
 - sh run command, 471–472
 - show ip protocol (sh ip protocol) command, 469–471
- RIPng (RIP Next Generation), 499–500**
- [rip_tag] tags, 500**
- RIPv2 (Routing Information Protocol version 2), 474–475**
 - configuring, 466–468
 - route configuration, 473–474
- RIR (Regional Internet Registries), 315, 529**
- RJ-45 connectors, 40, 70–71, 75, 255**
- roaming, WLAN connectivity, 178**
- role separation, 728**
- rollover cabling, 255–256**
- root DNS servers, 539–540**
- Root Guard, 636**
- route flapping, 478**
- route print command, 448**
- router ospf [process id] command, 481**
- routers**
 - access, 626–628
 - administrative distance, 461
 - auto-negotiation, 383–386
 - auxiliary input, 250
 - configure terminal (conf t) command, 374
 - configuring
 - Privileged EXEC mode (Router#), 380–381*
 - User EXEC mode (Router>), 369–371*
 - console input/cabling, 250
 - console ports
 - console cabling, 255*
 - DB-9 connectors, 254–255*
 - DB-25 connectors, 254, 255*
 - PuTTY software, 256–259*
 - RJ-45 connectors, 255*
 - rollover cabling, 255–256*

- RS-232 serial communications ports*, 254, 255
- serial interfaces*, 256
- ZTerm serial communications software*, 259–261
- enable command, 373
- enable secret command, 375
- EXEC (privileged EXEC) passwords, 627
- FastEthernet interface configurations, 376–377
- FastEthernet ports, 250, 263
- fundamentals of, 358–364
- gateway addresses, 265
- higher-end routers, VoIP, 252–253
- home networks, 26–27
- hostname command, 374–375
- interconnecting LAN, 262–266
- interfaces, 250–251
 - administratively down*, 390
 - auto-negotiation*, 383–386
 - full-duplex mode*, 384–386
 - troubleshooting*, 387–392
- ip helper command, 533
- line console passwords, 375–376
- line passwords, 626–627
- logging, 630–631
- logical addresses, 249
- MPLS, 252
- network addresses, 249
- no shutdown (no shut) command, 377
- packet shapers, 253
- ports, 249–250
- Privileged EXEC mode (Router#), 373–381
- privileged mode, 373
- QoS, 251–253
- Router (config-if)# prompt, 377
- routing tables, 265
- RSA keys, 627–628
- security, 626
 - access*, 626–628
 - logging*, 630–631
 - services*, 628–630
- segments, 265–266
- serial interfaces, 251, 377–380
- serial ports, 264
- services, 628–630
- show ip interface brief (sh ip int brief) command, 377, 387–392, 430
- uptime, 369
- USB interfaces, 250
- User EXEC mode (Router>), 366–371
- VIC-4FXS/DID, 251
- voice interface cards, 251
- VoIP, 251
- WIC2AM, 251
- wireless routers, 25, 28, 213
- routing**
 - advertising, 466
 - BGP, 496–498, 501–502
 - CIDR, 329
 - blocks*, 330–331
 - IPv6 addressing*, 337–338
 - notation*, 329
 - subnet mask conversions*, 329–330
 - distance vector protocols, 463
 - hop count metrics*, 463–464
 - RIP*, 465
 - RIP, [rip_tag] tags*, 500
 - RIP, configuring*, 466–468
 - RIP, IPv6*, 499–500
 - RIP, route configuration*, 468–473
 - RIP, sh run command*, 471–472
 - RIP, show ip protocol (sh ip protocol) command*, 469–471
 - RIP and link state protocols*, 477
 - RIPv2*, 474–475
 - RIPv2, configuring*, 466–468
 - RIPv2, route configuration*, 473–474
 - routing loops*, 465
 - dynamic routing protocols, 460, 461
 - convergence*, 460
 - load balancing*, 460
 - metrics*, 460, 461
 - path determination*, 460
 - EIGRP, 487–494, 501
 - GRE, 648–649
 - IPv6 routing, 499
 - BGP*, 501–502
 - EIGRP*, 501
 - OSPF*, 500–501
 - RIP*, 499–500
 - static routing*, 499
 - link state protocols, 476–477
 - configuring*, 481–485
 - EIGRP*, 487–494

- EIGRP, IPv6, 501
- IS-IS, 478–479
- LSA, 477
- NET addresses, 479
- OSPF, 477, 483–486
- OSPF, advantages/disadvantages of, 478
- OSPF, Area 0, 482
- OSPF, areas, 477
- OSPF, hello packets, 477
- OSPF, IPv6, 500–501
- OSPF, router ospf [process id] command, 481
- OSPF, VLSM, 478
- RIP and, 477
- route flapping, 478
- loops, 465
- OSPF, 477
 - advantages/disadvantages of, 478
 - areas, 477
 - hello packets, 477
 - VLSM, 478
- RIP, 465
- RIPng, 499–500
- static routing, 447–448, 458
 - commands (overview), 457
 - configuring, 454–458
 - copy running-configuration startup-configuration (copy run start) command, 457
 - default gateways, 448
 - gateways of last resort, 454
 - ip route command, 451
 - IPv6, 499
 - loopbacks, 448–449
 - netstat -r command, 448
 - route print command, 448
 - routing tables, code C, 453
 - routing tables, code S, 453
 - setting, 449–451
 - show ip route (sh ip route) command, 451–454
 - show ip route static (sh ip route static) command, 456
 - show running-config (sh run) command, 456–457
 - show startup-config (sh start) command, 457
 - subnet masks, 451
 - VLSM, 451
 - write memory (wr m) command, 457
- wire speed routing, 247

- routing tables**
 - code C, 453
 - code S, 453
 - defined, 265
- RPO (Recovery Point Objectives), 732**
- RR (Resource Records), DNS, 541–546**
- RS-232 serial communications ports, 254, 255**
- RSA keys, 627–628**
- RSL (Received Signal Levels), fiber-optic cabling, 142**
- RSSI (Received Signal Strength Indicators), 214**
- RSTP (Rapid Spanning Tree Protocol), 423–424**
- RTO (Recovery Time Objectives), 732**
- rules/regulations**
 - industry regulatory compliance, 718
 - FERPA, 718
 - FISMA, 719
 - GDPR, 719
 - GLBA, 719–720
 - HIPAA, 720
 - international export controls, 720–722
 - PCI DSS, 720
 - safety codes/standards
 - biometric scanners, 717
 - CFR, 709–716
 - Design and Construction Requirements for Exit Routes (29 CFR 1910.36), 709–710
 - door access, 717
 - Emergency Action Plans (29 CFR 1910.38), 710–711
 - Employee Alarm Systems (29 CFR 1910.165), 715–716
 - Fire Detection Systems (29 CFR 1910.164), 714–715
 - Fire Prevention Plans (29 CFR 1910.39), 711–712
 - Fixed Extinguishing Systems (29 CFR 1910.160), 713–714
 - Hazard Communication (29 CFR 1910.1200), 716
 - HVAC systems, 717
 - Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37), 710
 - MSDS, 716
 - NFPA, 709
 - OSH Act, 708–709
 - OSHA, 708–709
 - Portable Fire Extinguishers (29 CFR 1910.157), 712–713
 - SDS, 716
- runts, 433**

S

SaaS (Software as a Service), 695

safety

codes/standards

- biometric scanners*, 717
- CFR*, 709–716
- Design and Construction Requirements for Exit Routes (29 CFR 1910.36)*, 709–710
- door access*, 717
- Emergency Action Plans (29 CFR 1910.38)*, 710–711
- Employee Alarm Systems (29 CFR 1910.165)*, 715–716
- Fire Detection Systems (29 CFR 1910.164)*, 714–715
- Fire Prevention Plans (29 CFR 1910.39)*, 711–712
- Fixed Extinguishing Systems (29 CFR 1910.160)*, 713–714
- Hazard Communication (29 CFR 1910.1200)*, 716
- HVAC systems*, 717
- Maintenance, Safeguards, and Operational Features for Exit Routes (29 CFR 1910.37)*, 710
- MSDS*, 716
- NFPA*, 709
- OSH Act*, 708–709
- OSHA*, 708–709
- Portable Fire Extinguishers (29 CFR 1910.157)*, 712–713
- SDS*, 716

fiber-optic cabling, 127, 160–161

SAN (Storage Area Networks), 698–699

- FC*, 699
- FCoE*, 699
- IB*, 699
- iSCSI*, 699

sanitizing devices for disposal, 662

SC connectors, fiber-optic cabling, 145–146

scalability, cloud computing, 695–696

scaling networks, 537–538

scanners, biometric, 661, 717

scattering, fiber-optic cabling, 136

screened subnets, 618

SDN (Software-Defined Networking), 696–697

SDS (Safety Data Sheets), 716

SD-WAN (Software-Defined Wide Area Networks), 697

secure addresses, switches, 243

security

- 3DES, 651
- access control, 659, 660–661
 - access control vestibules (mantraps)*, 661
 - badge readers*, 661
 - biometric scanners*, 661
 - locking cabinets*, 661
 - locking racks*, 661
- AH, 651
- analog modems, 643–644
- antivirus/anti-malware software, 610–611
- ARP cache poisoning, 598
- Bluetooth, 641
- botnets, 608
- brute-force attacks, 596
- buffer overflow attacks, 599–600
- cable modems, 644
- change management policies, 624
- cloud computing, 697
- computer forensics, 621
- content filters, 620
- coordinated DDoS attacks, 608
- DAI, 635
- DDoS attacks, 608–609
- deauthentication/disassociation attacks, 608
- DES, 651
- dictionary attacks, 596
- Diffie-Hellman key exchange, 651
- directed broadcasts, 607
- documentation, 624
- DoS attacks, 606–609
- DTLS protocol, 598
- encryption, 33
- ESP, 651
- evil twin attacks, 598
- EXEC (privileged EXEC) passwords, 627
- fiber-optic cabling, 127
- firewalls, 34
 - ACL*, 617–618
 - configuring*, 611–617
 - deploying*, 619
 - DMZ*, 618
 - NGFW*, 620

- packet filtering*, 618
- personal firewalls*, 610
- proxy servers*, 618
- screened subnets*, 618
- SPI*, 34
- stateful firewalls*, 618
- home networks, 33–34
- IDS, 619
- IKE, 651
- intrusion attacks, 594–604
- IoT, 662–663
- IP security cameras, 662
- IPS, 619
- IPSec, 598, 651
- ISAKMP, 651
- Kerberos authentication, 623
- locks, racks, 73
- logic bombs, 604
- MAC addresses, filtering, 33
- malware, 602–604, 610–611
- modems
 - analog modems*, 643–644
 - cable modems*, 644
 - xDSL modems*, 644–646
- NAC, 624
- NAT, 34
 - defined*, 34
 - private IP addresses*, 34–35
 - public IP addresses*, 35
- network access management, 623–624
- on-path attacks (man-in-the-middle attacks), 598
- packet sniffing attacks, 597–599
- passwords
 - changing factory passwords*, 33
 - cracking attacks*, 596–597
- PDoS attacks, 607
- physical security, 659, 660
 - access control*, 659, 660–661
 - access control vestibules (mantraps)*, 661
 - asset disposal*, 662
 - badge readers*, 661
 - biometric scanners*, 661, 717
 - control devices*, 660
 - detection methods*, 661–662
 - door access*, 717
 - locking cabinets*, 661
 - locking racks*, 661
 - motion detection*, 662
 - surveillance*, 659
 - surveillance cameras*, 662
 - testing*, 659
- RADIUS, 624
- ransomware attacks, 604
- RAS, 647
- RBAC, 623
- reflective/amplified DoS attacks, 608
- remote access security, 642
 - analog modems*, 643–644
 - cable modems*, 644
 - RAS*, 647
 - xDSL modems*, 644–646
- routers, 626
 - access*, 626–628
 - logging*, 630–631
 - services*, 628–630
- RSA keys, 627–628
- session hijacking, 599
- smart doorbells, 663
- smart lockers, 663
- smart speakers, 663
- smart thermostats, 663
- social engineering attacks, 595–596
- software
 - buffer overflow attacks*, 599–600
 - netstat -a command*, 600
 - netstat -b command*, 601
 - nmap command*, 601–602
 - penetration testing*, 602
 - vulnerabilities*, 599–604
- SPI, 34
- spoofing attacks, 607, 635
- SSID
 - changing default SSID*, 33
 - turning off SSID broadcasts*, 33
- SSL protocol, 597–598
- switches, 631–633
 - BPDU Filter*, 636
 - BPDU Guard*, 635–636
 - DAI*, 635
 - ports*, 633–635
 - Root Guard*, 636
 - STP*, 635–636

- TACACS+624
- TLS protocol, 598
- TTLS protocol, 598
- Type 5 encryption algorithm, 627
- Type 7 encryption algorithm, 627
- UTM, 624
- viruses, 602–603, 610–611
- VLAN hopping, 599
- VPN, 34
 - CHAP, 649, 650
 - client-to-site VPN, 648
 - EAP, 650
 - GRE, 648–649
 - headends, 647
 - IP tunnels, 648
 - IPSec, 651
 - L2F, 650
 - L2TP, 650
 - MD5 hashing algorithm, 649, 650
 - mGRE, 649
 - PAP, 649–650
 - PPP, 649
 - PPTP, 650
 - remote access VPN, 648
 - remote client configurations, 652–657
 - SHA, 649, 650
 - site-to-site VPN, 648
 - tunneling protocols, 648–651
- web filters, 620
- wireless networks (Wi-Fi), 637
 - AES, 640
 - Bluetooth, 641
 - CCMP, 639–640
 - EAP, 640, 650
 - guidelines, 640–641
 - hotspots, 641
 - jamming, 638
 - LEAP, 640
 - Open Authentication, 638
 - RADIUS, 640
 - shared-key authentication, 638
 - SSID, 638
 - TKIP, 639
 - war chalking, 641
 - war driving, 641
 - war flying, 641
- WEP, 638–639
- WPA, 639
 - WPA2, 639–640
 - WPA3, 640
- WLAN, 637
 - AES, 640
 - Bluetooth, 641
 - CCMP, 639–640
 - EAP, 640, 650
 - guidelines, 640–641
 - hotspots, 641
 - jamming, 638
 - LEAP, 640
 - Open Authentication, 638
 - RADIUS, 640
 - shared-key authentication, 638
 - SSID, 638
 - TKIP, 639
 - war chalking, 641
 - war driving, 641
 - war flying, 641
 - WEP, 638–639
 - WPA, 639
 - WPA2, 639–640
 - WPA3, 640
- worms, 603
- xDSL modems, 644–646
- zero-day attacks, 604
- segments, 265–266**
 - defined, 246
 - subnet, NET, 363
- semi-active RFID tags, 202**
- serial interfaces**
 - console ports, routers, 256
 - HSSI, 270
 - routers, 251, 377–380
- serial ports, 264**
- servers**
 - proxy servers, 618
 - RAS, 647
 - root DNS, 539–540
- service attributes, Ethernet, 276–277**
- services**
 - cloud services, 692–693
 - DaaS, 695
 - DSL, 645

- IaaS, 694
- MSA, 724
- PaaS, 695
- routers, 628–630
- SaaS, 695
- xDSL, 645
- session hijacking, 599**
- Session layer, OSI model, 13**
- setting up (configuring)**
 - BGP, 496–498
 - computers for LAN operation, 44
 - EIGRP, 488–494
 - FastEthernet interfaces, 376–377
 - firewalls, 611–617
 - interfaces, auto-negotiation, 383–386
 - IP addressing, switches, 245
 - OSPF, 481–485
 - PuTTY software, 256–259
 - routers
 - Privileged EXEC mode (Router#), 380–381*
 - User EXEC mode (Router>), 369–371*
 - SLAAC, 336–337
 - SNMP, 547–551
 - static routing, 454–458
 - static VLAN, 414–418
 - switches, 410, 419–420
 - configure terminal (conf t) command, 411*
 - enable secret command, 412*
 - hostname command, 411–412*
 - line console passwords, 412–414*
 - privileged mode, 411, 412*
 - static VLAN configurations, 414–418*
 - switch# prompt, 412*
 - switch(config)# prompt, 411, 412*
 - switch(config-line)# prompt, 413*
 - VLAN subinterfaces, 418–419*
 - virtualization, 682–690
 - WLAN, 185–195, 206–211
- SFP (Small Form-Factor Pluggables), 152–153**
- SFP+153–154**
- SFTP (Secure File Transfer Protocol), 566**
- sh run command, 471–472**
- SHA (Secure Hash Algorithm), 649, 650**
- shared-key authentication, 638**
- “shooting the fiber”, 162**
- show flash command, 368**
- show interface status (sh int status) command, 430–431**
- show ip interface brief (sh ip int brief) command, 377, 387–392, 430**
- show ip protocol (sh ip protocol) command, 469–471**
- show ip route (sh ip route) command, 451–454**
- show ip route static (sh ip route static) command, 456**
- show mac address-table command, 433–434**
- show running-config command, 429–430**
- show running-config (sh run) command, 456–457**
- show startup-config (sh start) command, 457**
- show version command, 368–369, 434**
- signal strength, WLAN, 191–195**
 - RF site surveys, 209–211
 - RSSI, 214
 - troubleshooting, 214
- signal transmission, 10GBASE-T cabling, 100–101**
- single-mode fibers, 130, 134–135**
- site surveys, 190–195, 207, 209–211**
- site-to-site VPN, 648**
- SLA (Service-Level Agreements), 693, 724**
- SLAAC (Stateless Address Autoconfiguration), 336–337**
- Slotted Aloha, 203**
- slowdowns, network, 233**
- sm (single-mode) fibers, 155**
- smart devices, 568**
- smart doorbells, 663**
- smart lockers, 663**
- smart speakers, 663**
- smart thermostats, 663**
- snapshots**
 - virtualization, 681
 - WLAN, 192–193
- SNMP (Simple Network Management Protocol), 546–547**
 - configuring, 547–551
 - MIB, 547
 - SNMPv2, 550
 - SNMPv3, 550
- snooping, DHCP, 572**
- SOA (Start of Authority) resource records, 541**
- social engineering attacks, 595–596**
- software**
 - antivirus/anti-malware software, 610–611
 - botnets, 608
 - buffer overflow attacks, 599–600
 - coordinated DDoS attacks, 608
 - DDoS attacks, 608–609

- deauthentication/disassociation attacks, 608
- directed broadcasts, 607
- DoS attacks, 606–609
- logic bombs, 604
- malware, 602–604
- PDoS attacks, 607
- ransomware attacks, 604
- reflective/amplified DoS attacks, 608
- SDN, 696–697
- security
 - netstat -a* command, 600
 - netstat -b* command, 601
 - nmap* command, 601–602
 - penetration testing*, 602
- spoofing attacks, 607
- viruses, 602–603
- vulnerabilities, 599–604
- worms, 603
- zero-day attacks, 604
- SONET/SDH (Synchronous Optical Networks/
Synchronous Digital Hierarchy), 148**
 - hierarchy data rates, 149
 - STS, 149
- SOP (Standard Operating Procedures), 726–727**
- source-quench packets, 302**
- SOW (Statements of Work), 725**
- spatial diversity, 186**
- speakers, smart, 663**
- speeds, data, home networks, 30**
- SPF (Sender Policy Frameworks), 544**
- SPI (Stateful Pack Inspection), 34**
- splicing**
 - connectorization, 146
 - fusion splicing, 144
 - index-matching gel, 144
 - mechanical splicing, 144–145
- splitters, fiber-optic cabling, 142**
- spoofing attacks, 607, 635**
- spot-the-difference troubleshooting approach, 569**
- SRV records (Service records), 544**
- SSID (Service Set Identifiers), 186, 638**
 - broadcasts, turning off, 33
 - changing, 33
 - defined, 33
 - troubleshooting, 215
- SSL (Secure Socket Layer) protocol, 597–598**
- ST connectors, fiber-optic cabling, 145–146**
- stacked switches, 243–244**
- star topologies, 9, 10, 39**
- start frame delimiters, defined, 17**
- stateful firewalls, 618**
- static assignments, 243**
- static routing, 447–448, 458**
 - commands (overview), 457
 - configuring, 454–458
 - copy running-configuration startup-configuration (copy run start) command, 457
 - default gateways, 448
 - gateways of last resort, 454
 - ip route command, 451
 - IPv6, 499
 - loopbacks, 448–449
 - netstat -r command, 448
 - route print command, 448
 - routing tables
 - code C*, 453
 - code S*, 453
 - setting, 449–451
 - show ip route (sh ip route) command, 451–454
 - show ip route static (sh ip route static) command, 456
 - show running-config (sh run) command, 456–457
 - show startup-config (sh start) command, 457
 - subnet masks, 451
 - VLSM, 451
 - write memory (wr m) command, 457
- static VLAN, 408, 414–418**
- step-index fiber, 133**
- sticky command option, 634**
- storage**
 - NAS, 700
 - SAN, 698–699
- store-and-forward mode, switches, 246**
- STP (Shielded Twisted-Pair) cabling, 76–77**
- STP (Spanning Tree Protocol), 422–424**
 - BPDU Filter, 636
 - BPDU Guard, 635–636
 - Root Guard, 636
- straight-through cabling, 82, 87–90**
- straight-through ports, 42**
- strands, fiber-optic cabling, 131–132**

stretching cable, 102**structured cabling**

- backbone cabling, 67
- building entrances, 66–67
- ER, 67
- HC, 68, 69
- horizontal cabling, 67, 69–73
- IC, 68, 69
- MC, 68, 69
- STP cabling, 76–77
- TCO, 67
- telecommunications closets, 67, 69–70
- TIA/EIA 568-A cabling standard, 66
- TIA/EIA 568-B cabling standard, 66
- TIA/EIA 569B cabling standard, 66–67
- twisted-pair cabling, 74, 78–80
- UTP cabling, 74–76
- WO, 68
- work areas, 67

STS (Synchronous Transport Signals), 149**subinterfaces, VLAN, 418–419****subnet masks**

- ANDing, 361–362
- applying, 318
- CIDR-subnet mask conversions, 329–330
- classful addresses, 317
- creating, 321
- defined, 317
- examples of, 324–326
- magic numbers, 323
- original/default subnet masks, 319
- static routing, 451
- subnetting process, 319–323
- troubleshooting, 570–571
- VLSM, 331–332, 451, 478

subnetting

- broadcast addresses, 322
- classful addresses, 317
- defined, 318–319
- magic numbers, 323
- NET, 363
- network addresses, 322
- network numbers, 482
- process of, 319–323
- VLSM, 331–332

supernetting, 328–329

- CIDR, 329–330
- CIDR blocks, 330–331
- VLSM, 331–332

surveillance

- cameras, 662
- physical security, 659

switches, 9, 237–238, 239, 410

- adaptive cut-through mode, 247
- aging time, 244
- benefits of, 246
- BPDU, 422–423
- broadcast domains, 246
- CNA, 242–243
- collisions, 433
- configure terminal (conf t) command, 411
- configuring, 411, 412, 419–420
- connections, 10
- CRC errors, 432
- cut-through mode, 247
- dynamic assignments, 243
- enable secret command, 412
- error thresholds, 247
- fast-forward mode, 247
- flooding, 246
- fragment-free mode, 247
- giants, 433
- home networks, 26
- hostname command, 411–412
- hubs and, 10, 239–242
- input errors, 432
- IP addressing, 245
- isolating collision domains, 246
- latency, 246
- layer 2 switches, 238
- line console passwords, 412–414
- link light indicators, 42
- managed switches, 242–247
- MLS, 247
- multicast messages, 239
- PD, 426, 427
- PoE, 425–428
- PoE+427
- PoE++428
- ports, 243, 431–432, 633–635
- privileged mode, 411, 412

- PSE, 426–427
- runts, 433
- secure addresses, 243
- security, 631–633
 - BPDU Filter*, 636
 - BPDU Guard*, 635–636
 - DAI*, 635
 - ports*, 633–635
 - Root Guard*, 636
 - STP*, 635–636
- show interface status (sh int status) command, 430–431
- show mac address-table command, 433–434
- show running-config command, 429–430
- show version command, 434
- stacked switches, 243–244
- static assignments, 243
- static VLAN, configuring, 414–418
- store-and-forward mode, 246
- STP, 422–424
- switch# prompt, 412
- switch(config)# prompt, 411, 412
- switch(config-line)# prompt, 413
- troubleshooting, 429–434
- VLAN
 - security*, 634
 - subinterfaces*, 418–419
 - wire speed routing, 247
- SYN (Synchronizing) packets, 297**
- SYN ACK (Synchronizing Acknowledgement) packets, 297**
- system labeling, 72**

T

T1 to T3 data rates, 270

T568A wiring standard

- color maps, 78–80
- defined, 78
- pinouts, 79

T568B wiring standard

- color maps, 78–80
- defined, 78
- pinouts, 79

TACACS+ (Terminal Access Controller Access-Control System Plus), 624

tag-based VLAN, 408

tags

- RFID, 200
 - active tags*, 202
 - communications (air interface) portal*, 203
 - frequency bands*, 203
 - HF tags*, 203
 - LF tags*, 203
 - passive tags*, 201–202
 - semi-active tags*, 202
 - Slotted Aloha*, 203
 - UHF tags*, 203
- [rip_tag] tags, 500
- VLAN tags, 277

TCL (Transverse Conversion Loss), 99

TCO (Telecommunications Outlets), 67

TCP (Transmission Control Protocol), 292

- defined, 297
- headers, 296–297
- packets
 - terminating connections*, 299–300
 - transmitting*, 298
- ports, 573
- three-packet TCP handshakes, 298, 299

TCP/IP (Transmission Control Protocol/Internet Protocol), 21–22

- Application layer, 294, 295–296
- defined, 292
- gateway addresses, 326–327
- Internet layer, 294, 301
 - ARP*, 301–303
 - ICMP*, 302–303
 - IGMP*, 303–304
 - IP*, 301
- IPv4 addressing, 312–313
 - 6to4 prefix*, 335
 - ARIN*, 315
 - assigning*, 315
 - classes*, 313
 - classful addresses*, 317
 - decimal/binary octets*, 314
 - dual stacks*, 336
 - host IP addresses*, 315
 - network/host bits*, 314–315
 - non-Internet-routable IP addresses*, 316
 - private IP addresses*, 316
 - RIR*, 315

- structure of, 313*
 - transitioning to IPv6, 335–337*
- IPv6 addressing, 333–335
 - 6to4 prefix, 335*
 - anycast addresses, 335*
 - CIDR, 337–338*
 - DAD, 337*
 - defined, 333*
 - dual stacks, 336*
 - interface (host) identifiers, 335*
 - IPng, 333*
 - link-local addresses, 335, 336–337*
 - multicast addresses, 335*
 - SLAAC, 336–337*
 - transitioning to, 335–337*
 - unicast addresses, 335*
- layers of, summary, 294
- Network interface layer, 294, 304
- number conversions
 - binary-to-decimal conversions, 306–307*
 - decimal-to-binary conversions, 307–309*
 - hexadecimal numbers, 309–311*
- ports, 295
- subnet masks
 - ANDing, 361–362*
 - applying, 318*
 - CIDR-subnet mask conversions, 329–330*
 - classful addresses, 317*
 - creating, 321*
 - defined, 317*
 - examples of, 324–326*
 - magic numbers, 323*
 - original/default subnet masks, 319*
 - subnetting process, 319–323*
- subnetting
 - broadcast addresses, 322*
 - classful addresses, 317*
 - defined, 318–319*
 - magic numbers, 323*
 - network addresses, 322*
 - process of, 319–323*
 - VLSM, 331–332*
- supernetting, 328–329
 - CIDR, 329–330*
 - CIDR blocks, 330–331*
 - VLSM, 331–332*
- Transport layer, 294, 296–301

- TCTL (Transverse Conversion Transfer Loss), 99**
- TE (Telecommunications Enclosures), structured cabling, 67**
- teaming, NIC, 18**
- telco, defined, 270**
- telco clouds, 270–271**
- telecommunications closets**
 - components of, 69–70
 - structured cabling, 67
- terminating**
 - cabling, 70
 - CAT6 horizontal cabling, 83–87*
 - TCP connections, 299–300*
 - twisted-pair cabling, 78–80*
 - DTX-1800 certification reports, 103, 104
- testing**
 - cabling, 92–93
 - ACR, 93, 95*
 - attenuation (insertion loss), 92, 93–94*
 - channel specifications, 93–96*
 - delay skew, 93, 96*
 - ELFEXT, 93, 95*
 - near-end testing, 94*
 - NEXT, 92, 93, 94–95*
 - propagation delay, 93, 96*
 - PSACR, 93, 95, 96*
 - PSELFEXT, 93, 95, 96*
 - PSNEXT, 93, 94*
 - return loss, 93, 95–96*
 - LAN, 45–48
 - near-end testing, 94
 - physical security, 659
- thermostats, smart, 663**
- Thin/Net cabling, bus topologies, 8**
- three-packet TCP handshakes, 298, 299**
- TIA (Telecommunications Industry Alliance)**
 - defined, 66
 - TIA/EIA 568-A cabling standard, 66
 - TIA/EIA 568-B cabling standard, 66
 - TIA/EIA 569B cabling standard, 66–67
- ticks metrics, 461**
- time, aging, 244**
- TKIP (Temporal Key Integrity Protocol), 639**
- TLD (Top-Level Domains), 539**
- TLS (Transport Layer Security) protocol, 598**
- Token Ring hubs, 7**
- Token Ring topologies, 6, 7–8**

- tokens, passing, 7**
- topologies, 7**
 - bus topologies, 8–9
 - campus network hierarchical topologies, 69
 - defined, 6
 - hub-and-spoke topologies. *See* star topologies
 - mesh topologies, 10–11
 - point-to-point topologies, 6
 - star topologies, 9, 10, 39
 - Token Ring topologies, 6, 7–8
- top-to-bottom (top-down) troubleshooting approach, 569**
- TR (Telecommunications Rooms), structured cabling, 67**
- traffic analysis, 552–565**
- traffic filtering, 268**
- traffic flows**
 - CBS, 276
 - CIR, 276
 - EBS, 276
 - EIR, 276
 - LAN, 269
- transceivers**
 - optical networking, 154
 - WLAN, 177
- translation bridges, 235**
- transmission strands, fiber-optic cabling, 126**
- transmit power**
 - 802.11a (Wi-Fi 2) wireless standard, 181
 - WLAN, 180
- transmitting data, long hauls, 134**
- transparent bridges, 235**
- transport input none command, 627**
- Transport layer**
 - OSI model, 13
 - protocol, 296
 - TCP/IP, 294, 296–301
- tree hierarchies, DNS, 539–540**
- troubleshooting**
 - AP, 213
 - bottom-to-top (bottom-up) approach, 569
 - cabling, 102
 - DTX-1800 certification reports, 103, 104*
 - failures to meet manufacturer specifications, 102–104*
 - multimeters, 110*
 - performance, 110*
 - stretching, 102*
 - WLAN, 215*
 - channel utilization, WLAN, 214–215
 - compatibility (wireless), 213
 - connectivity, 110
 - deauthentication/disassociation attacks, 215
 - DHCP, 216, 571–572
 - divide-and-conquer approach, 569
 - fiber-optic cabling, 162–163
 - gateways, 571
 - home networks, 31–32
 - IP addresses, 570
 - IP networks, 568–573
 - LAN, 45–48
 - load issues (WLAN), 215
 - name resolution, 571
 - networks
 - bottom-to-top (bottom-up) approach, 569*
 - divide-and-conquer approach, 569*
 - isolating problems, 14*
 - spot-the-difference approach, 569*
 - top-to-bottom (top-down) approach, 569*
 - ping command, 14
 - printers, 216
 - router interfaces, 387–392
 - signal strength, WLAN, 214
 - spot-the-difference approach, 569
 - SSID, 215
 - subnet masks, 570–571
 - switches, 429–434
 - TCP ports, 573
 - top-to-bottom (top-down) approach, 569
 - UDP ports, 573
 - wired networks, 31–32
 - wireless networks (Wi-Fi), 31–32, 213
 - AP, 213*
 - cabling, 215*
 - channel utilization, 214–215*
 - compatibility, 213*
 - deauthentication/disassociation attacks, 215*
 - DHCP, 216*
 - extending wireless ranges, 214*
 - frequencies, 214*
 - interference, 214*
 - load issues, 215*
 - signal strength, 214*
 - SSID, 215*
 - wireless printers, 216*

- wireless routers*, 213
- WPA, 215
- wireless printers, 216
- wireless routers, 213
- WLAN. *See* wireless networks (Wi-Fi)
- trunk ports**, 408–409
- TTLS (Tunneled Transport Layer Security) protocol**, 598
- tunable lasers**, 141–142
- tunneling protocols**
 - L2F, 650
 - L2TP, 650, 651
 - PPTP, 650
 - VPN, 648–651
- turning off SSID broadcasts**, 33
- twisted-pair cabling**. *See also* physical layer cabling
 - ELTCTL, 99
 - F/UTP, 99
 - LCL, 99
 - return loss, 93, 95–96
 - STP cabling, 76–77
 - TCL, 99
 - TCTL, 99
 - terminating, 78–80
 - UTP cabling
 - CAT3, 75, 76
 - CAT5, 74, 75, 76
 - CAT5e, 74, 75, 76, 79–82
 - CAT6, 74, 75, 76, 79–82
 - CAT6a, 75, 76
 - CAT7, 74, 75, 79–82
 - CAT7a, 75
 - CAT8, 74, 75, 79–82
- “two-deep” rule, optical networking**, 152–153
- TXT records (Text records)**, 544
- Type 1 hypervisors**, 680
- Type 2 hypervisors**, 680
- Type 5 encryption algorithm**, 627
- Type 7 encryption algorithm**, 627

U

- UDP (User Datagram Protocol)**
 - defined, 300
 - headers, 300–301
 - packet transfers, 300–301
 - ports, 573

- UHF (Ultra-High Frequency) RFID tags**, 203
- unconnected fibers, fiber-optic cabling**, 146
- UNI (User-Network Interfaces)**, 274
- unicast addresses**, 335, 533
- U-NII (Unlicensed-National Information Infrastructure)**, 802.11a (Wi-Fi 2) wireless standard, 180–181
- UPC connectors**, 64, 146
- uplink ports**, 42
- uptime, routers**, 369
- USB interfaces**, 250
- User EXEC mode (Router>)**, 366–371
- UTM (Unified Threat Management)**, 624
- UTP (Unshielded Twisted-Pair) cabling**
 - CAT3, 75, 76
 - CAT5, 74, 75, 76
 - patch cabling*, 87–90
 - straight-through cabling*, 87–90
 - CAT5e, 74, 75, 76, 79–82
 - patch cabling*, 87–90
 - straight-through cabling*, 87–90
 - test examples*, 104–109
 - CAT6, 74, 75, 76, 79–82, 83–87
 - CAT6a, 75, 76
 - CAT7, 74, 75, 79–82
 - CAT7a, 75
 - CAT8, 74, 75, 79–82
 - F/UTP, 99
- UTP couplers**, 64

V

- V.44/V.34 modem standard**, 643
- V.92/V.90 modem standard**, 643
- VCSEL (Vertical Cavity Surface Emitting Lasers)**, 141
- verifying**
 - network connections with ping command, 240–241
 - network settings, 570
- VFL (Visual Fault Locators)**, 162
- VIC-4FXS/DID**, 251
- virtual desktops, remote desktops and**, 695
- virtualization**, 679, 682
 - 32-bit CPU architectures, 679
 - 64-bit CPU architectures, 679
 - advantages/disadvantages of, 680–681
 - caches, 679
 - cores, 679

- defined, 679
- disaster recovery, 681
- dongles, 682
- guest machines, 680
- hardware keys, 682
- host machines, 680
- Hyper-V, 682–690
- hypervisors, 680
- Live Migration, 681
- SD-WAN, 697
- setting up, 682–690
- snapshots, 681
- VM, 680, 681–682
- vMotion, 681
- XenMotion, 681

viruses, 602–603, 610–611

VLAN (Virtual Local Area Networks), 407.
See also LAN

- assigning memberships, 408
- dynamic VLAN, 408
- hopping, 599
- port assignments, 431
- port-based VLAN, 407
- protocol-based VLAN, 408
- PVST, 423–424
- static VLAN, 408, 414–418
- subinterfaces, 418–419
- switch security, 634
- tag-based VLAN, 408
- tags, 277, 408–409
- trunk ports, 408–409
- VSTP, 423–424
- VTP, 409

VLSM (Variable-Length Subnet Masking), 331–332

- OSPF, 478
- static routing, 451

VM (Virtual Machines), 680, 681–682

vMotion, 681

voice gateways, 251

voice interface cards, 251

VoIP (Voice Over Internet Protocol)

- jitter, 252
- networks
- congestion (bottlenecking), 252
 - latency, 252*
- QoS, 251–253

- queuing/buffering, 252
- routers, 251, 252–253

VPN (Virtual Private Networks), 34

- CHAP, 649, 650
- client-to-site VPN, 648
- EAP, 650
- GRE, 648–649
- headends, 647
- IP tunnels, 648
- IPSec, 651
- L2F, 650
- L2TP, 650
- MD5 hashing algorithm, 649, 650
- mGRE, 649
- PAP, 649–650
- PPP, 649
- PPTP, 650
- remote access VPN, 648
- remote client configurations, 652–657
- SHA, 649, 650
- site-to-site VPN, 648
- tunneling protocols, 648–651

VSTP (VLAN Spanning Tree Protocol), 423–424

VTP (VLAN Trunking Protocol), 409

W

WAN (Wide Area Networks), 5

- defined, 526
- example of, 526
- HSSI, 270
- interconnecting LAN, 267–277
- OC, 270
- SD-WAN, 697

war chalking, 641

war driving, 641

war flying, 641

warm sites, disaster recovery, 731

WDM (Wavelength Division Multiplexing), 130, 143

- diplexers, 154
- transceivers, 154

web filters, 620

well-known (reserved) ports, 295

WEP (Wired Equivalent Privacy), 638–639

whois command, 530

WIC2AM (WAN Interface Cards), 251

- Wi-Fi 1 (802.11b) wireless standard, 24, 181, 183**
- Wi-Fi 2 (802.11a) wireless standard, 24, 180–181, 183**
- Wi-Fi 3 (802.11g) wireless standard, 24, 181, 182, 183**
- Wi-Fi 4 (802.11n) wireless standard, 24, 181, 182, 183**
- Wi-Fi 5 (802.11ac) wireless standard, 24, 182, 183**
- Wi-Fi 6 (802.11ax) wireless standard, 25, 182, 183**
- Wi-Fi Alliance, 24–25, 183**
- Wi-Fi networks. *See* wireless networks (Wi-Fi)**
- wildcard bits, 482–483**
- WiMAX (Worldwide Interoperability for Microwave Access), 199–200**
- Windows 10**
 - command prompt, 18
 - firewalls, 611–615
 - home networks, connecting, 32
 - MAC addresses, obtaining, 20
 - PuTTY software, 256–259
 - remote client VPN configurations, 652
- wire speed routing, 247**
- wired networks**
 - access points (AP), 28
 - advantages/disadvantages of, 24
 - appearance, 31
 - broadband modems/gateways, 28
 - cable modems, 28, 29
 - components of, 25–30
 - cost, 30
 - data speeds, 30
 - defined, 24
 - DSL modems, 29–30
 - ease of implementation, 31
 - example of, 25
 - home access, 31
 - hubs, 25
 - network adapters, 26
 - public access, 31
 - routers, 26–27
 - switches, 26
 - troubleshooting, 31–32
 - wireless routers, 28
- wireless bridges, 187–189, 236**
- wireless controllers, 189**
- wireless LAN adapters, 185**
- wireless networks (Wi-Fi), 24, 174**
 - 3G wireless standard, 204
 - 4G wireless standard, 204
 - 5G wireless standard, 204
 - 802.11 wireless standard, 175–176
 - MAC layer, 176*
 - PHY layer, 176*
 - 802.11a (Wi-Fi 2) wireless standard, 180–181, 183
 - 802.11ac (Wi-Fi 5) wireless standard, 182, 183
 - 802.11ax (Wi-Fi 6) wireless standard, 182, 183
 - 802.11b (Wi-Fi 1) wireless standard, 181, 183
 - 802.11g (Wi-Fi 3) wireless standard, 181, 182, 183
 - 802.11i wireless standard, 183
 - 802.11n (Wi-Fi 4) wireless standard, 181, 182, 183
 - 802.11r wireless standard, 183
 - 802.16a (WiMAX) wireless standard, 200
 - access points (AP), 28
 - ad hoc networks, 176, 177
 - advantages/disadvantages of, 24
 - AES, 640
 - ANT+ wireless technology, 183
 - antennas, 186
 - dish (parabolic reflector) antennas, 209*
 - EIRP, 210*
 - extending wireless ranges, 214*
 - multipoint distributions, 209–211*
 - omnidirectional antennas, 208–209*
 - placement of, 207*
 - remote installations, 211*
 - RF site surveys, 209–211*
 - selecting, 208–209*
 - site surveys, 207*
 - Yagi antennas, 209*
 - AP, 177–178, 186–187, 189–190
 - appearance, 31
 - associations, 186–187, 193
 - basic setup, 185–186
 - beacons, 638
 - beamforming, 182
 - Bluetooth
 - BLE technology, 197*
 - enabling connections, 198–199*
 - inquiry procedures, 197*
 - output power classes, 197*
 - paging procedures, 197*
 - piconets, 197–198*
 - security, 641*
 - broadband modems/gateways, 28
 - BSS, 176, 177, 178
 - BWA, 199–200
 - cable modems, 28, 29

- cabling, troubleshooting, 215
- captive portals, 32
- CCMP, 639–640
- CDMA, 204
- channel bonding, 179
- channel utilization, 214–215
- components of, 25–30
- configuring, 185–195, 206–211
- connecting, 32
- cost, 30
- CSMA/CD, 178
- data speeds, 30
- deauthentication/disassociation attacks, 215
- defined, 24, 174
- device density, 189
- DHCP, 216
- distance, 189–190
- DSL modems, 29–30
- DSSS, 179
- EAP, 640, 650
- ease of implementation, 31
- EDGE, 204
- encryption, 33
- ESS, 178
- example of, 25
- FHSS, 180
- firewalls, 34
- frequencies, troubleshooting, 214
- frequency channels, 179
- geofencing, 204
- hand-offs, 178
- home access, 31
- hopping sequences, 180
- hotspots, 32, 641
- HSPA+204
- hubs, 25
- IEEE wireless standards, 24–25
- interference, troubleshooting, 214
- IP addressing, 34–36
- ISM band, 179
- last-mile connections, 200
- LEAP, 640
- load issues, troubleshooting, 215
- loss of association, 193
- LTE/4G, 204
- MIMO, 182
- mobile (cellular) communications, 204
- MU-MIMO, 182
- NAT, 34
 - defined, 34*
 - private IP addresses, 35*
 - public IP addresses, 35*
- network adapters, 26
- NFC, 204
- OFDM, 180
- point-to-multipoint WLAN configuration case study, 206–211
- printers, 216
- pseudorandom numbering sequences, 180
- public access, 31
- RADIUS, 640
- ranges (wireless), extending, 32, 195, 214
- RFID, 200, 201
 - backscatter, 200*
 - block diagram, 200–201*
 - inlays, 202*
 - readers, 201*
 - tags, 200, 201–203*
- roaming, 178
- routers, 26–27
- RSSI, 214
- security, 33–34, 637
 - AES, 640*
 - Bluetooth, 641*
 - CCMP, 639–640*
 - EAP, 640, 650*
 - guidelines, 640–641*
 - hotspots, 641*
 - jamming, 638*
 - LEAP, 640*
 - Open Authentication, 638*
 - RADIUS, 640*
 - shared-key authentication, 638*
 - SSID, 638*
 - TKIP, 639*
 - war chalking, 641*
 - war driving, 641*
 - war flying, 641*
 - WEP, 638–639*
 - WPA, 639*
 - WPA2, 639–640*
 - WPA3, 640*

- signal strength, 191–195, 214
- site surveys, 190–195, 207, 209–211
- snapshots, 192–193
- spatial diversity, 186
- SSID, 186, 215
- switches, 26
- transceivers, 177
- transmit power, 180
- troubleshooting, 31–32, 213
 - AP, 213
 - cabling, 215
 - channel utilization, 214–215
 - compatibility, 213
 - deauthentication/disassociation attacks, 215
 - DHCP, 216
 - extending wireless ranges, 214
 - frequencies, 214
 - interference, 214
 - load issues, 215
 - signal strength, 214
 - SSID, 215
 - wireless printers, 216
 - wireless routers, 213
 - WPA, 215
- VPN, 34
- war chalking, 641
- war driving, 641
- war flying, 641
- Wi-Fi Alliance, 24–25, 183
- WiMAX, 199–200
- wireless bridges, 187–189
- wireless controllers, 189
- wireless LAN adapters, 185
- wireless routers, 25, 28
- wireless standards, 32
- WLC, 189–190
- WMN, 176
- WPA, 215, 639
- WPA2, 639–640
- WPA3, 640
- Z-Wave wireless technology, 183
- wireless printers, troubleshooting, 216**

- wireless routers, 25, 28**
 - home networks, 28
 - troubleshooting, 213
- wireless standards**
 - 802.1x (dot1x) wireless standard, 633
 - 802.11 wireless standard, 175–176
 - ad hoc networks*, 176, 177
 - AP, 177–178
 - BSS, 176, 177, 178
 - channel bonding, 179
 - CSMA/CD, 178
 - DSSS, 179
 - ESS, 178
 - FHSS, 180
 - frequency channels, 179
 - hand-offs, 178
 - hopping sequences, 180
 - ISM band, 179
 - MAC layer, 176
 - OFDM, 180
 - Open Authentication, 638
 - PHY layer, 176
 - pseudorandom numbering sequences, 180
 - roaming, 178
 - shared-key authentication, 638
 - transceivers, 177
 - transmit power, 180
 - WMN, 176
 - 802.11a (Wi-Fi 2) wireless standard, 24, 180–181, 183
 - 802.11ac (Wi-Fi 5) wireless standard, 24, 182, 183
 - 802.11ax (Wi-Fi 6) wireless standard, 25, 182, 183
 - 802.11b (Wi-Fi 1) wireless standard, 24, 181, 183
 - 802.11g (Wi-Fi 3) wireless standard, 24, 181, 182, 183
 - 802.11i wireless standard, 183
 - 802.11n (Wi-Fi 4) wireless standard, 24, 181, 182, 183
 - 802.11r wireless standard, 183
 - 802.16a (WiMAX) wireless standard, 200
 - wireless networks (Wi-Fi), 32
- wiremaps, 82**
- Wireshark, network traffic analysis, 560–565**
- wiring standards**
 - T568A wiring standard
 - color maps*, 78–80

- defined*, 78
- pinouts*, 79
- T568B wiring standard
 - color maps*, 78–80
 - defined*, 78
 - pinouts*, 79
- WLAN (Wireless Local Area Networks), 174.**
 - See also* LAN**
 - 3G wireless standard, 204
 - 4G wireless standard, 204
 - 5G wireless standard, 204
 - 802.11 wireless standard, 175–176
 - MAC layer*, 176
 - PHY layer*, 176
 - 802.11a (Wi-Fi 2) wireless standard, 180–181, 183
 - 802.11ac (Wi-Fi 5) wireless standard, 182, 183
 - 802.11ax (Wi-Fi 6) wireless standard, 182, 183
 - 802.11b (Wi-Fi 1) wireless standard, 181, 183
 - 802.11g (Wi-Fi 3) wireless standard, 181, 182, 183
 - 802.11i wireless standard, 183
 - 802.11n (Wi-Fi 4) wireless standard, 181, 182, 183
 - 802.11r wireless standard, 183
 - 802.16a (WiMAX) wireless standard, 200
 - ad hoc networks, 176, 177
 - AES, 640
 - ANT+ wireless technology, 183
 - antennas, 186
 - dish (parabolic reflector) antennas*, 209
 - EIRP*, 210
 - extending wireless ranges*, 214
 - multipoint distributions*, 209–211
 - omnidirectional antennas*, 208–209
 - placement of*, 207
 - remote installations*, 211
 - RF site surveys*, 209–211
 - selecting*, 208–209
 - site surveys*, 207
 - Yagi antennas*, 209
 - AP, 177–178, 186–187, 189–190
 - associations, 186–187, 193
 - basic setup, 185–186
 - beacons, 638
 - beamforming, 182
 - Bluetooth
 - BLE technology*, 197
 - enabling connections*, 198–199
 - inquiry procedures*, 197
 - output power classes*, 197
 - paging procedures*, 197
 - piconets*, 197–198
 - security*, 641
 - BSS, 176, 177, 178
 - BWA, 199–200
 - cabling, troubleshooting, 215
 - CCMP, 639–640
 - CDMA, 204
 - channel bonding, 179
 - channel utilization, 214–215
 - configuring, 185–195, 206–211
 - CSMA/CD, 178
 - deauthentication/disassociation attacks, 215
 - defined, 174
 - device density, 189
 - DHCP, 216
 - distance, 189–190
 - DSSS, 179
 - EAP, 640, 650
 - EDGE, 204
 - ESS, 178
 - FHSS, 180
 - frequencies, troubleshooting, 214
 - frequency channels, 179
 - geofencing, 204
 - hand-offs, 178
 - hopping sequences, 180
 - hotspots, 641
 - HSPA+204
 - interference, troubleshooting, 214
 - ISM band, 179
 - last-mile connections, 200
 - LEAP, 640
 - load issues, troubleshooting, 215
 - loss of association, 193
 - LTE/4G, 204
 - MIMO, 182

- mobile (cellular) communications, 204
- MU-MIMO, 182
- NFC, 204
- OFDM, 180
- point-to-multipoint WLAN configuration case study, 206–211
- printers, 216
- pseudorandom numbering sequences, 180
- RADIUS, 640
- range extenders, 195
- ranges (wireless), extending, 214
- RFID, 200, 201
 - backscatter*, 200
 - block diagram*, 200–201
 - inlays*, 202
 - readers*, 201
 - tags*, 200, 201–203
- roaming, 178
- RSSI, 214
- security, 637
 - AES*, 640
 - Bluetooth*, 641
 - CCMP*, 639–640
 - EAP*, 640, 650
 - guidelines*, 640–641
 - hotspots*, 641
 - jamming*, 638
 - LEAP*, 640
 - Open Authentication*, 638
 - RADIUS*, 640
 - shared-key authentication*, 638
 - SSID*, 638
 - TKIP*, 639
 - war chalking*, 641
 - war driving*, 641
 - war flying*, 641
 - WEP*, 638–639
 - WPA*, 639
 - WPA2*, 639–640
 - WPA3*, 640
- signal strength, 191–195, 214
- site surveys, 190–195, 207, 209–211
- snapshots, 192–193
- spatial diversity, 186
- SSID, 186, 215
- transceivers, 177
- transmit power, 180
- troubleshooting, 213
 - AP*, 213
 - cabling*, 215
 - channel utilization*, 214–215
 - compatibility*, 213
 - deauthentication/disassociation attacks*, 215
 - DHCP*, 216
 - extending wireless ranges*, 214
 - frequencies*, 214
 - interference*, 214
 - load issues*, 215
 - signal strength*, 214
 - SSID*, 215
 - wireless printers*, 216
 - wireless routers*, 213
 - WPA*, 215
- war chalking, 641
- war driving, 641
- war flying, 641
- Wi-Fi Alliance, 183
- WiMAX, 199–200
- wireless bridges, 187–189
- wireless controllers, 189
- wireless LAN adapters, 185
- WLC, 189–190
- WMN, 176
- WPA, 215, 639
- WPA2, 639–640
- WPA3, 640
- Z-Wave wireless technology, 183
- WLC (Wireless LAN Controllers), 189–190**
- WMN (Wireless Mesh Networks), 176**
- WO (Work-Area Outlets), 68**
- work areas, 67**
- worms, 603**
- WPA (Wi-Fi Protected Access), 215, 639**
- WPA2 (Wi-Fi Protected Access version 2), 639–640**
- WPA3 (Wi-Fi Protected Access version 3), 640**
- write memory (wr m) command, 457**
- WSN (Wireless Sensor Networks), ANT+ wireless technology, 183**

X

X2, 153–154

xDSL

modems, security, 644–646

services, 645

XenMotion, 681

XENPAK, 153–154

XFP, 153–154

XPAK, 153–154

Y

Yagi antennas, 209

Z

zero-day attacks, 604

zero dispersion wavelengths, 138–139

**ZTerm serial communications software, configuring,
259–261**

Z-Wave wireless technology, 183